

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE CIÊNCIAS ECONÔMICAS
DEPARTAMENTO DE ECONOMIA E RELAÇÕES INTERNACIONAIS

DANIEL BRYK SILVEIRA

BITCOIN:
CONCORRÊNCIA OU COOPERAÇÃO À MOEDA TRADICIONAL?

Porto Alegre

2016

DANIEL BRYK SILVEIRA

**BITCOIN:
CONCORRÊNCIA OU COOPERAÇÃO À MOEDA TRADICIONAL?**

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para a obtenção do título de Bacharel em Ciências Econômicas.

Orientador: Prof. Dr. Antônio Ernani Martins
Lima

Porto Alegre

2016

DANIEL BRYK SILVEIRA

BITCOIN: CONCORRÊNCIA OU COOPERAÇÃO À MOEDA TRADICIONAL?

Trabalho de conclusão submetido ao Curso de Graduação em Ciências Econômicas da Faculdade de Ciências Econômicas da UFRGS, como requisito parcial para a obtenção do título de Bacharel em Ciências Econômicas.

Aprovada em: Porto Alegre, 30 de novembro de 2016.

BANCA EXAMINADORA:

Prof. Dr. Antônio Ernani Martins Lima - Orientador

UFRGS

Prof. Dr. Ronald Otto Hillbrecht

UFRGS

Prof. Dr. Eugenio Lagemann

UFRGS

RESUMO

A revolução tecnológica na área da computação e da Internet trouxe modificações importantes nos mais variados setores da sociedade. Atualmente, a maioria das transações financeiras ocorre virtualmente, nesse contexto surgiu a moeda digital Bitcoin. O conceito desta moeda foi introduzido em 2008 e pode ser descrito como a primeira criptomoeda descentralizada do mundo. As transações em Bitcoin ocorrem sem a necessidade de um intermediário e não dependem da confiança em nenhum emissor centralizado ou instituição financeira. Ao longo deste trabalho serão expostas as características, o funcionamento, as vantagens e desvantagens desta nova moeda, contrastando-a à moeda tradicional de cunho forçado. O objetivo principal é observar se essa nova tecnologia pode ser uma alternativa concorrente aos meios tradicionais, até o ponto de substituir por completo as moedas usadas nos dias de hoje, centralizadas em bancos centrais, ou se a criptomoeda será uma aliada cooperativa à moeda tradicional. Conclui-se que o Bitcoin é no curto e médio prazo uma moeda paralela, ou seja, que coopera e é aliada aos meios tradicionais.

Palavras-chave: Bitcoin. Criptomoeda. Dinheiro virtual. Moeda. Economia Monetária.

Classificação JEL: E42 – Sistemas monetários; Padrões; Regimes; Governos e o sistema monetário; Sistemas de pagamento.

ABSTRACT

The technological revolution in the field of computing and the Internet has brought important changes in many sectors of society. Currently, most financial transactions take place virtually, in this context came out the digital currency Bitcoin. The concept was introduced in the year of 2008 and can be described as the first decentralized cryptocurrency in the world. The transactions occur without the need of an intermediary and do not depend on any centralized trusted issuer or financial institution. Throughout this written essay, it will be exhibited the characteristics, operation, advantages and disadvantages of Bitcoin, comparing with the traditional currency. The main aim is to observe if this new technology can be a competitive alternative to the traditional methods, to the point of completely replace the coins used nowadays, concentrated on central banks, or if the cryptocurrency will be an ally cooperative to traditional currency. The conclusion is that the Bitcoin is in short and medium term a parallel currency, that means, is an ally and cooperate with the traditional methods.

Keywords: Bitcoin. Cryptocurrency. Currency. Virtual money. Monetary Economy.

JEL Classification: E42 – Monetary systems; Standards; Regimes; Government and the monetary system; Paymentsystems.

SUMÁRIO

1 INTRODUÇÃO	6
1.1 Questão a investigar	7
1.2 Objetivos	7
1.2.1 Objetivo geral	7
1.2.2 Objetivos específicos	7
1.3 Justificativa e importância do estudo	8
1.4 Metodologia	8
2 ANÁLISE DA MOEDA E DO DINHEIRO	10
2.1 Evolução e história do dinheiro	10
2.2 As funções da moeda e suas características essenciais	12
2.3 Evolução dos tipos de moeda	14
2.4 Agregados monetários	18
3 UM ESTUDO SOBRE O BITCOIN	20
3.1 Contexto e surgimento	20
3.2 Funcionamento e características	23
3.3 Outras moedas digitais	31
4 ANÁLISE DO BITCOIN	32
4.1 Vantagens e desvantagens do uso do Bitcoin	32
4.2 Análise de dados	36
4.3 Aceitação do Bitcoin	42
4.4 Bitcoin é moeda?	45
4.5 Regulação	48
5 CONCLUSÃO	51
6 REFERÊNCIAS	54

1 INTRODUÇÃO

A revolução científica e tecnológica que se apresenta na sociedade nos últimos séculos criou novas oportunidades e soluções em todas as áreas do conhecimento. A última grande revolução tecnológica foi a da computação e da Internet. É unicamente através dessas inovações que foi possível a criação de uma moeda criptografada e descentralizada. Nesse contexto surgiu a mais famosa das criptomoedas, o Bitcoin, que pode ser entendido como a primeira criptomoeda descentralizada da história. É um sistema de pagamento online baseado em protocolo de código aberto, qualquer pessoa pode acessá-lo e sugerir modificações que julgue pertinente.

Atualmente as sociedades utilizam moedas centralizadas em bancos centrais e as transações online necessitam de um intermediador financeiro para ocorrer. O Bitcoin, ao contrário, não depende da confiança em nenhum órgão emissor ou instituição financeira. Bitcoin usa um banco de dados distribuídos espalhados pelos nós da rede *peer-to-peer*¹ para registrar as transações, e usa criptografia de código aberto para prover funções básicas de segurança, como certificar que Bitcoins só podem ser gastas pelo dono e evitar gastos duplos e falsificação.

A nova moeda pode ser uma alternativa à moeda convencional que é utilizada já há muitos séculos. Ela já pode ser considerada uma realidade e seus impactos na macroeconomia ainda são incertos e devem ser motivos de análise. A investigação do tema tem como objetivo observar se essa nova tecnologia pode ser uma alternativa concorrente aos meios tradicionais, até o ponto de substituir por completo as moedas usadas nos dias de hoje, centralizadas em bancos centrais, ou se a criptomoeda será uma aliada cooperativa à moeda tradicional.

Como as moedas criptografadas entraram em circulação não faz muito tempo, ainda não existem muitos estudos nessa área, e não há um consenso entre os estudiosos sobre a capacidade da moeda se consolidar nas economias nacionais. Há alguns textos e artigos científicos sobre o tema, entretanto ainda há muito espaço para debatê-lo.

¹ *Peer-to-peer* (do inglês *par-a-par* ou simplesmente ponto-a-ponto, com sigla P2P) é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

1.1 Questão a investigar

As principais questões a serem investigadas no presente trabalho podem ser resumidas em:

- Qual o funcionamento das moedas criptografadas?
- São concorrentes ou cooperam com a moeda tradicional?

1.2 Objetivos

1.2.1 Objetivo geral

O objetivo geral do trabalho é descrever o funcionamento das moedas criptografadas, em especial o Bitcoin, para analisar se elas são concorrentes ou cooperam com as moedas de cunho forçado. Isto é, se são uma ameaça e substituirão à moeda convencional ou se funcionam paralelamente e são aliadas às moedas centralizadas tradicionais. O Bitcoin, por ser a principal e mais utilizada das criptomoedas, será o foco da análise comparativa.

1.2.2 Objetivos específicos

Descrever historicamente o funcionamento das moedas tradicionais com o intuito de servir de base na comparação com as moedas digitais para responder à questão geral da monografia. O capítulo histórico-descritivo abordará esse assunto com ênfase na desmaterialização da moeda.

Como se dá o funcionamento de uma moeda criptografada, como o Bitcoin? Quais são suas principais características? Esse objetivo será tratado no capítulo teórico, que no presente estudo será o de número 3.

Identificar as vantagens e desvantagens da utilização desse tipo de moeda, para avaliar seu uso como alternativa aos meios tradicionais de pagamento. Objetivo explorado no capítulo de análise, que será o de número 4.

Também o capítulo de análise buscará explorar à seguinte questão: o Bitcoin pode ser considerado moeda de acordo com a teoria econômica?

1.3 Justificativa e importância do estudo

A criação de moedas criptografadas, como o Bitcoin, ainda é muito recente. O conceito foi introduzido em 2008 em um artigo publicado por um grupo de pessoas com o pseudônimo de Satoshi Nakamoto. Como o Bitcoin existe faz pouco tempo, ainda não há muitos estudos e trabalhos que busquem analisar o funcionamento e os impactos dessa nova moeda. Logo, a importância acadêmica do tema é o fato de, com o desenvolvimento de novas tecnologias em diversas áreas, a moeda criptografada poder ser uma alternativa à moeda convencional que é utilizada já há muitos séculos.

As consequências e desdobramentos das moedas criptografadas ainda não foram dimensionados completamente. Ainda há muito o que se debater em relação às mesmas, por isso a importância do presente estudo.

Um fator importante na justificativa do estudo é o fato de estarmos vivendo um processo de desmaterialização da moeda, a partir do avanço da tecnologia digital e da comunicação via internet. Assim, as moedas criptografadas podem ocupar um nicho em um cenário possível do fim do uso da moeda de papel. A Suécia, por exemplo, segundo projeções de seu Banco Central, prevê o fim do uso de cédulas e moedas até 2030, segundo matéria da BBC em 12 de abril de 2016.

1.4 Metodologia

O presente trabalho será composto de três partes. A primeira parte será dedicada à revisão teórica de o que é moeda, quais são suas características, sua evolução e a sua importância para o funcionamento e desenvolvimento da economia. A segunda parte será utilizada para explicar como se dá o funcionamento da moeda criptografada Bitcoin, quais são suas principais características e por que ela está sendo considerada tão revolucionária. Na terceira parte serão comparadas as moedas tradicionais e a criptografada Bitcoin com o objetivo de responder às principais questões levantadas. As moedas criptografadas, mas em especial o Bitcoin, poderão cooperar ou serão concorrentes da moeda tradicional? Ela pode ser considerada uma ameaça às moedas tradicionais, ou seja, poderá, no futuro, substituir a moeda como a conhecemos, centralizadas em bancos centrais?

O método adotado será a utilização de pesquisa explanatória, analisando fatos históricos através da leitura de ampla bibliografia. Como instrumento de pesquisa, será utilizada a pesquisa bibliográfica e a consulta de fontes secundárias. Como a quantidade de trabalhos acadêmicos na área ainda é relativamente restrita, serão utilizadas como fontes, informações buscadas em páginas da internet, nos documentos divulgados pelos próprios sistemas de moedas virtuais e nos relatórios de órgãos e entidades governamentais.

2 ANÁLISE DA MOEDA E DO DINHEIRO

2.1 Evolução e história do dinheiro

Há muito tempo, no período dos caçadores e coletores, o dinheiro não existia. Cada grupo caçava, coletava e produzia quase tudo que necessitava, desde carnes a roupas e até medicamentos. Diferentes membros do bando podiam se especializar em diferentes tarefas, mas compartilhavam seus bens e serviços em uma economia de favores e obrigações. Um pedaço de carne fornecido de graça levava consigo a suposição de reciprocidade – por exemplo, assistência medicinal gratuita. Os bandos internamente eram economicamente independentes, e as trocas quase não existiam. A exceção eram alguns itens raros que não podiam ser encontrados localmente, precisavam ser obtidos com outros grupos. Essas trocas eram realizadas por meio de escambo simples. Trocava-se uma quantidade do bem X por outra do bem Y (HARARI, 2015).

Até mesmo após o início da revolução agrícola, a maioria das pessoas continuou morando em comunidades pequenas e íntimas. Da mesma forma que os grupos de caçadores-coletores, cada aldeia constituía-se em uma unidade econômica autossuficiente, mantida por obrigações e favores mútuos, além de um pouco de escambo com outros grupos. Existia um pouco de especialização. Por exemplo, um indivíduo podia fazer sapatos, outro fornecia cuidados médicos. Desse modo, seus vizinhos sabiam a quem recorrer quando ficavam descalços ou doentes. Mas os povoados eram pequenos e suas economias eram limitadas, por isso não podia haver sapateiros e médicos em tempo integral (HARARI, 2015).

Com o desenvolvimento de cidades e reinos e a melhora considerável da infraestrutura de transporte, novas oportunidades de especialização surgiram. Cidades densamente povoadas ofereciam empregos em tempo integral não só para sapateiros e médicos profissionais como também para carpinteiros, sacerdotes, soldados e advogados. Com isso as economias foram se especializando e uma nova gama de profissões foi surgindo (HARARI, 2015).

Entretanto, a especialização criou um novo problema: como gerenciar a troca de bens e serviços entre os diferentes tipos de profissionais? Uma economia baseada em favores e obrigações não funciona, quando grandes números de estranhos tentam cooperar. Uma coisa é fornecer assistência gratuita para um familiar ou amigo; outra é cuidar de estranhos que podem nunca retribuir o favor. O escambo até pode suprir essa dificuldade, mas ele só é eficiente, quando se troca uma gama limitada de produtos. Não serve para formar a base de uma economia diferenciada e complexa (HARARI, 2015).

O dinheiro foi criado muitas vezes, em muitos lugares. Seu desenvolvimento não exigiu nenhum progresso tecnológico: foi uma revolução puramente mental. Necessitou da criação de uma nova realidade intersubjetiva que existe apenas na imaginação coletiva das pessoas. Dinheiro não são apenas moedas e cédulas.

Dinheiro é qualquer coisa que as pessoas estejam dispostas a usar para representar sistematicamente o valor de outras coisas com o propósito de trocar bens e serviços. O dinheiro permite que as pessoas comparem de maneira fácil e rápida o valor de diferentes mercadorias (como maçãs, sapatos e divórcios), troquem uma coisa pela outra com facilidade e armazenem riqueza de forma conveniente (HARARI, 2015, p. 185).

A moeda é, portanto, um meio universal de troca que permite que as pessoas convertam quase tudo em praticamente qualquer outra coisa. Por ser capaz de converter, armazenar e transportar riqueza de maneira fácil e barata, a moeda fez uma contribuição vital ao surgimento de redes comerciais complexas e mercados dinâmicos. Sem ela, os mercados e redes comerciais teriam sido fadados a permanecer muito limitados em tamanho, complexidade e dinamismo (HARARI, 2015).

As moedas só têm valor em nossa imaginação coletiva. Seu valor não surge da estrutura química, cor ou forma das conchas e do papel. Ou seja, dinheiro não é uma realidade material, e sim um construto psicológico. Mas só tem êxito, pois as pessoas só estão dispostas a fazer essas coisas quando confiam no produto da imaginação coletiva. A confiança é a matéria-prima com que todos os tipos de dinheiro são cunhados (HARARI, 2015).

O dinheiro é um sistema de confiança mútua, e não só isso: o dinheiro é o mais universal e mais eficiente sistema de confiança mútua já inventada. O que criou essa confiança foi uma complexa rede de relações políticas, sociais e econômicas de longo prazo (HARARI, 2015).

O papel fundamental da confiança explica por que os sistemas financeiros são tão intimamente relacionados aos sistemas político, social e ideológico. Também esclarece o porquê de as crises financeiras, com frequência, serem desencadeadas por processos políticos e o mercado de ações pode subir ou cair dependendo de como os executivos se sentem naquela manhã em particular. Inicialmente, quando as primeiras versões de moedas foram criadas, as pessoas não tinham esse tipo de confiança, então era necessário definir como moeda coisas que tinham valor real intrínseco. A primeira forma de dinheiro conhecida na história foram os grãos de cevada utilizados pelos sumérios. Apareceu na Suméria, por volta de 3000 a.C. no mesmo período e lugar, e sob as mesmas circunstâncias, do aparecimento da escrita. Assim como a escrita se desenvolveu para atender às necessidades de se intensificar as atividades

administrativas, o dinheiro de cevada se desenvolveu para atender às necessidades de se intensificar as atividades econômicas (HARARI, 2015).

No fim da era moderna, o planeta inteiro era uma única zona monetária, primeiro baseada em ouro e prata e depois em algumas moedas confiáveis como a libra esterlina e o dólar americano. O aparecimento de uma só zona monetária transnacional e transcultural deu origem às bases para a unificação da Afro-Ásia, e, com o tempo, do mundo inteiro, em uma única esfera econômica e política. As pessoas continuaram a falar línguas diferentes, obedecer a governantes diferentes e adorar deuses distintos, mas todos acreditavam em ouro e prata e em moedas de ouro e de prata. Sem essa crença compartilhada, as redes de comércio mundiais teriam sido praticamente impossíveis. O ouro e a prata que os conquistadores do século XVI acharam na América permitiram que os mercadores europeus comprassem seda, porcelana e especiarias no leste da Ásia, estimulando o crescimento econômico tanto na Europa quanto no leste da Ásia (HARARI, 2015).

O dinheiro é baseado em dois princípios universais: a convertibilidade universal e confiança universal, com o dinheiro como intermediário, quaisquer duas pessoas podem cooperar em qualquer projeto. Esses princípios permitiram que milhões de estranhos cooperassem no comércio e na indústria de maneira eficaz.

2.2 As funções da moeda e suas características essenciais

A moeda surgiu com o objetivo de facilitar a troca de bens e serviços entre os indivíduos da sociedade. Para isso, uma moeda deve exercer três principais funções: meio ou instrumento de troca, unidade de conta e reserva de valor (MONTORO FILHO & TROSTER, 2004).

Meio ou instrumento de troca é a função que pode ser compreendida quando pensamos como seria a sociedade atual se não tivesse um meio de troca aceito por todos. Sem moeda, todas as trocas deveriam ser diretas, ou seja, como ocorre com o escambo. Assim, um sapateiro que desejasse comprar trigo deveria procurar um agricultor que desejasse comprar sapatos e com ele entrar em entendimento para fechar o negócio (MONTORO FILHO & TROSTER, 2004).

Ou seja, deveria ocorrer uma dupla coincidência de desejos, e ainda seria necessário resolver as questões da quantidade e da divisibilidade: quantos sapatos seriam necessários para comprar um saco de trigo ou vice-versa (MONTORO FILHO & TROSTER, 2004)?

A segunda função de uma moeda é ser unidade de conta. A moeda serve para comparar o valor de diversas mercadorias. Utilizando-a como denominador comum, é possível somar um

carro mais uma roupa e também achar sua equivalência em valor (MONTORO FILHO & TROSTER, 2004).

Logo, a unidade de conta pode ser usada contabilmente, sem necessidade de transferências físicas de moeda. O acerto de contas se processa apenas por expedientes contábeis, entrando a moeda simplesmente como unidade para essa contabilidade. A moeda também serve como unidade para pagamentos ao longo do tempo, para a realização de pagamentos no futuro (MONTORO FILHO & TROSTER, 2004).

A terceira função é ser reserva de valor. Para a moeda ser aceita em troca de mercadorias, é preciso que ela seja aceita também na compra de outros bens e serviços. Assim, a moeda representa um direito cujo seu possuidor tem sobre as mercadorias (MONTORO FILHO & TROSTER, 2004).

Uma pessoa a qual recebe uma moeda, não precisa gastá-la, imediatamente, podendo guardá-la para usar depois. Isso significa que ela serve como reserva de valor. A moeda, para executar bem essa função, deve ter valor estável, de forma que quem a possuir tenha ideia de quanto pode obter em troca. Mais de um ativo pode cumprir as funções da moeda, e, em algumas situações, a moeda oficial não cumpre perfeitamente todas as funções, principalmente em casos de alta inflação (MONTORO FILHO & TROSTER, 2004).

Para o bom desempenho das funções que foram expostas, a moeda deve apresentar algumas características essenciais. Durante a história da moeda, alguns atributos essenciais foram mantidos e, sem eles, os diferentes instrumentos monetários utilizados não poderiam cumprir as funções básicas que as configuram. Cabe destacar as mais relevantes: indestrutibilidade e inalterabilidade, homogeneidade, divisibilidade, transferibilidade e facilidade de manuseio e transporte.

A primeira característica é a da indestrutibilidade e inalterabilidade. A moeda deve possuir resistência. Não pode ser destruída ou se deteriorar com facilidade, ao longo de seu uso. Como exemplo, pode-se citar a busca de papéis de melhor qualidade para a impressão das moedas fiduciárias utilizadas nas transações. Esse atributo essencial também é obstáculo às falsificações, constituindo-se em elemento fundamental para a confiança das pessoas e na aceitação da moeda.

A moeda deve ser também homogênea. Duas unidades monetárias diferentes, mas de mesmo valor, devem ser exatamente iguais. Para exemplificar a necessidade de a moeda ser homogênea, supomos uma sociedade onde o arroz é utilizado como meio de troca. No caso, dois indivíduos realizam uma transação onde, o comprador paga a compra com o arroz de baixa qualidade e com grãos quebrados, enquanto o vendedor imagina que receberá, em troca de sua

mercadoria, grãos inteiros e de boa qualidade. É justamente pela possibilidade de isso ocorrer que é importante a moeda ser homogênea.

A terceira característica essencial para uma moeda é a divisibilidade. A moeda deve possuir valores múltiplos e submúltiplos em quantidade, de modo que tanto as transações de grande porte quanto as de pequeno porte possam ser realizadas sem dificuldade.

Já a transferibilidade, quarta característica, diz respeito à facilidade com que se deve processar a transferência de moeda de um indivíduo para outro. Esta característica tem a função de facilitar e de agilizar o processo de trocas na economia.

O quinto atributo de uma moeda é a facilidade de manuseio e transporte. As moedas têm como objetivo principal facilitar as trocas de bens e serviços entre as pessoas, e não o de dificultar. Se o porte da moeda for dificultado, sua utilização aos poucos seria descartada ou haveria um processo de substituição por uma mercadoria de transporte mais facilitado.

2.3 Evolução dos tipos de moeda

As primeiras moedas foram mercadorias. Estas deveriam ser raras e atender a uma necessidade comum e geral, para que pudessem ser aceitas por todos os indivíduos envolvidos em trocas indiretas. Desta forma, as primeiras moedas possuíam valor de uso. Uma vez este sendo comum e geral, passava também a possuir valor de troca. Com o passar do tempo, os instrumentos monetários foram sofrendo um processo lento e gradual de desmaterialização. A exigência do valor de uso foi progressivamente abandonada, enfatizando-se de forma crescente o valor de troca (LOPES & ROSSETTI, 1998).

Na antiguidade foram utilizadas como moeda-mercadoria: cobre, anéis de cobre, prata, cevada, gado, barras de ferro, espadas de ferro, escravos, animais domésticos, arroz, ouro, conchas, seda, instrumentos agrícolas e o sal.

Já na Idade Média as moedas de couro (precursoras das cédulas de papel), gado, ouro e prata em unidades-peso, cereais (arroz, aveia e centeio), mel, tecidos, peixes secos, escravos, manteiga, peles curtidas, chá, sal, peças de ferro, estanho, prata, anéis de cobre cobertos com ouro e prata e as pérolas foram alguns exemplos de mercadorias utilizadas como moeda.

Na Idade Moderna fumo, cereais, carnes-secas, madeira, gado, rum, trigo, carne, peles, metais preciosos e até o arroz também serviram como moeda-mercadoria (LOPES & ROSSETTI, 1998, p.30).

Apesar de terem chegado até a Idade Moderna, as moedas-mercadorias foram com o tempo sendo substituídas. A principal razão para a sua substituição por outras formas de moeda

foi que a maior parte das moedas-mercadorias não preenchia as características essenciais que se exigem dos instrumentos monetários para o desempenho de suas funções, o que comprometia sua aceitação geral (LOPES & ROSSETTI, 1998).

De forma geral, os metais foram as mercadorias que mais se ajustaram às funções monetárias, não apenas por satisfazer as características essenciais de uma moeda, como também porque seu valor de uso não compromete nem compete com seu valor de troca. A utilização de metais viabilizou o processo de cunhagem, que se certificava do peso e se garantia a sua circulação. Esse processo era realizado e administrado por chefes de estado e possibilitou a cobrança de tributos (LOPES & ROSSETTI, 1998).

Inicialmente, os metais mais utilizados e submetidos ao processo de cunhagem foram o cobre, o bronze e o ferro. Entretanto, como esses metais podiam ser encontrados com facilidade na natureza, eles não preenchiam algumas das condições necessárias para seu uso irrestrito como moeda, em especial servir como reserva de valor (LOPES & ROSSETTI, 1998).

Com o passar do tempo, os metais não nobres foram sendo substituídos pelo ouro e pela prata. Esses dois metais preciosos possuem características intrínsecas que satisfazem melhor os atributos essenciais que a moeda deve preencher. Como exemplo dessas características, pode-se citar o fato de que sempre foram muito procurados e desejados, seja pelo valor material, ou pelo valor simbólico. O ouro e a prata, enquanto instrumentos monetários, eram suficientemente escassos e as novas quantidades descobertas eram insignificantes em relação ao estoque existente, assim, seu valor se mantinha estável ao longo do tempo, confirmando a confiança dos indivíduos e favorecendo sua aceitação (LOPES & ROSSETTI, 1998).

O desenvolvimento de sistemas monetários à base de metais preciosos e o aumento das atividades comerciais e de produção abriram espaço para o aparecimento de um novo tipo de moeda, a moeda-papel (LOPES & ROSSETTI, 1998).

Com o desenvolvimento das trocas entre regiões cada vez mais distantes, o transporte das moedas metálicas era bastante complicado, devido ao peso e ao risco de roubos. Para minimizar essas dificuldades desenvolveram-se esforços para a criação e a difusão de moedas mais flexíveis (LOPES & ROSSETTI, 1998).

Particularmente após o Renascimento, os comerciantes, forçados por essas circunstâncias, passaram a recorrer a instituições que, por força de suas funções, estavam equipadas para guardar, sob garantia, metais monetários e outros valores. Essas eram chamadas de casas de custódia, que passaram a custodiar ouro e prata, fornecendo aos depositantes certificados de depósito, que por comodidade e segurança, começaram a circular no lugar dos metais monetários. Como tinham lastro de 100% e garantia de conversibilidade, já que seus

detentores podiam trocá-las pelos metais depositados, essa garantia, acabou transformando-se em uma nova moeda e em instrumento de troca e reserva de valor (LOPES & ROSSETTI, 1998).

O uso generalizado da moeda-papel propiciou o desenvolvimento de uma nova modalidade de moeda não integralmente lastreada. A experiência da custódia e da conversibilidade mostrou que lastro metálico integral, em relação aos certificados em circulação, não era necessário para o pleno funcionamento do novo sistema monetário. Já que a reconversão da moeda-papel em metais preciosos não era solicitada por todos os detentores ao mesmo tempo. Enquanto uns solicitavam reconversão, outros levavam às casas de custódia, nova quantidades de ouro e prata, dando origem a novas emissões (LOPES & ROSSETTI, 1998).

Dessa forma, os responsáveis pelas casas de custódia, começaram a emitir certificados não lastreados. Esse processo significou a passagem da moeda-papel para o papel-moeda (moeda fiduciária). Em um primeiro estágio o papel-moeda possui lastro inferior a 100% e menor garantia de conversibilidade. Quando todos resolviam converter seus certificados pelos metais, verificava-se uma “quebra geral do sistema”. Para evitar isso, os Estados passaram a regulamentar as emissões com intuito de diminuir o risco sistêmico. O sistema de cobertura integral, o sistema de reserva proporcional e o sistema de teto máximo formam os três sistemas básicos que norteavam o sistema financeiro com o objetivo de torná-lo mais estável (LOPES & ROSSETTI, 1998).

Entretanto, essas medidas não foram suficientes, pois com a grande crise de 1929 esses esforços se mostraram inúteis, tendo sido abandonada a ideia de conversão. A partir de então, com exceção do dólar, que manteve até 1971 a tradição e a garantia do lastro metálico proporcional, as moedas deixaram de ter garantias metálicas. Atualmente, os sistemas monetários são fiduciários e de curso forçado, tendo como propriedades a inexistência de lastro metálico, a inconvertibilidade absoluta e o monopólio estatal das emissões (LOPES & ROSSETTI, 1998).

Junto da moeda fiduciária, de emissão não lastreada e monopolizada pelo Estado, de curso forçado e de poder liberatório garantido por disposições legais, desenvolve-se outra modalidade de moeda: a moeda bancária, escritural ou invisível (LOPES & ROSSETTI, 1998).

Hoje em dia, moeda bancária representa a maior parcela dos meios de pagamento, segundo o conceito convencional de moeda, na maioria dos países. Esse tipo de moeda é criado pelos bancos detentores de depósitos à vista e a prazo e corresponde ao total desses depósitos nesses estabelecimentos. Sua movimentação é realizada por cheques ou por ordens de

pagamento, hoje em dia normalmente através de transferências eletrônicas. A moeda bancária é também conhecida por ser invisível, pois não tem existência física, e é escritural, por corresponder apenas a lançamentos de débito e crédito, registrados nas contas correntes dos bancos (LOPES & ROSSETTI, 1998).

As formas mais comuns de moeda utilizadas atualmente (moeda fiduciária e moeda bancaria) constituem apenas valor de troca. Integralmente desmaterializadas, não apresentam nenhuma utilidade para a direta satisfação das necessidades humanas (LOPES & ROSSETTI, 1998).

Os avanços tecnológicos, principalmente o desenvolvimento da informática e da internet facilitaram ainda mais as trocas monetárias. Atualmente, as moedas tornaram-se um conjunto de registros eletrônicos representativos de outros ativos. A maioria das transações ocorre em terminais de autoatendimento ou por meio da internet, diminuindo consideravelmente o uso da moeda em papel e auxiliando no processo de desmaterialização da mesma. A chamada moeda eletrônica consiste em unidades de moeda nacional armazenadas em dispositivos eletrônicos, que podem ser utilizados em transações no mundo digital (PREVIDI, 2014; BACEN, 2014).

Nos dias atuais as moedas e cédulas são uma forma rara de dinheiro. A soma de todo o dinheiro do mundo é de cerca de 60 trilhões de dólares, mas a soma total de moedas e cédulas é de menos de 6 trilhões de dólares. Mais de 90% de todo o dinheiro – mais de 50 trilhões de dólares que aparecem em nossas contas – existem apenas em servidores de computador. Assim, a maior parte das transações é executada por meio da movimentação de dados eletrônicos de um arquivo de computador para outro, sem qualquer troca de dinheiro físico. Na verdade, enquanto as pessoas estiverem dispostas a trocar bens e serviços por dados eletrônicos, será algo ainda melhor do que moedas e cédulas. Os dados eletrônicos são mais leves, ocupam menos espaço e são mais fáceis de controlar. O dinheiro, independentemente de sua forma, é condição essencial para sistemas comerciais complexos funcionarem (HARARI, 2015).

Assim, transações realizadas digitalmente estão ganhando força e podem até mesmo em um futuro não muito distantes acabar com uso de cédulas de papel e moedas metálicas. Sejam em sites de bancos, celulares ou máquinas de cartão de débito e crédito, a tecnologia proporciona todas as condições para que pagamentos, inclusive de pequenos valores possam ser feitas sem a necessidade de se portar dinheiro em espécie.

De acordo com notícia veiculada pelo site da BBC², até 2030 as cédulas e moedas deverão desaparecer na Suécia, a projeção conforme feita pelo Banco Central sueco. Os dados da autoridade monetária indicam que as transações em dinheiro representam, atualmente, apenas 2% do valor de todos os pagamentos realizados na Suécia – contra uma média de cerca de 7% no restante da Europa. A previsão é de que, no futuro, as economias modernas serão dominadas pelo uso do cartão e da moeda eletrônica em escala mundial.

2.4 Agregados monetários

O conceito do agregado monetário de meios de pagamento é utilizado para classificar o total de moeda de um país. Refere-se ao volume de dinheiro criado pelo Banco Central. Trata-se de uma definição restrita da oferta de dinheiro, que diz respeito apenas às formas mais líquidas.

No Brasil, como nos outros países, existem muitos ativos, como depósitos a prazo, bônus do Banco Central, caderneta de poupança, entre outros, que, apesar de não serem considerados moeda em sentido restrito, apresentam algumas características da moeda em sentido amplo. Esses ativos podem ser chamados de quase-moeda, pois podem, sem grandes problemas, ser transformados em moeda. São ativos de grande liquidez que apesar de não serem aceitos normalmente em troca de bens e serviços, podem rapidamente ser convertidos em moeda (MONTORO FILHO & TROSTER, 2004).

Cada país classifica os seus agregados monetários por ordem de liquidez. No Brasil, existem 5 agregados monetários: M0; M1; M2; M3; M4.

M0 e M1 são os meios de pagamento de liquidez imediata que não rendem juros. M0 é conhecido de moeda natural ou moeda corrente e é o estoque de moeda metálica e papel-moeda que fica em poder das pessoas ou das empresas, inclusive as reservas em moeda dos bancos. M1 são os depósitos em conta corrente nos bancos comerciais, conhecidos como moeda escritural ou bancária, mais o papel-moeda em poder do público (MONTORO FILHO & TROSTER, 2004).

M2, M3 e M4 incluem as quase-moedas que, por sua vez, rendem juros aos aplicadores (Figura 1).

² Matéria disponível

em: <http://www.bbc.com/portuguese/noticias/2016/04/160411_sociedade_sem_dinheiro_cw_rb>. Acesso em: 07/11/2016.

Figura 1 - Agregados monetários (meios de pagamento)

M0	Moeda em poder do público (papel-moeda e moedas metálicas) + reservas bancárias
M1	M0 + depósitos à vista nos bancos comerciais
M2	M1 + depósitos especiais remunerados + depósitos de poupança + títulos emitidos por instituições depositárias
M3	M2 + quotas de fundos de renda fixa + operações compromissadas registradas na Selic
M4	M3 + títulos públicos de alta liquidez

Fonte: MONTORO FILHO & TROSTER. Manual de Economia. p. 322, 2004.

O presente capítulo teve como objetivo caracterizar o funcionamento, o surgimento e a evolução da moeda. Após expor como e por que se desenvolveu o dinheiro, foram mostradas as principais características que um bem deve ter para ser considerado moeda. Foi visto também a evolução dos diversos tipos de moeda até chegar as moedas eletrônicas de hoje em dia. A revisão teórica apresentada teve como objetivo embasar a comparação das moedas tradicionais frente ao Bitcoin para dar luz às principais questões levantadas pelo trabalho.

3 UM ESTUDO SOBRE O BITCOIN

Nesse capítulo serão expostos o funcionamento e as principais características da criptomoeda Bitcoin. Apesar de existirem outras moedas criptografadas, o Bitcoin corresponde a quase 80% do volume financeiro presentes nesse tipo de ativo. Embora existam algumas diferenças entre as moedas digitais, o presente estudo enfocará especificamente no Bitcoin, que foi a primeira e continua sendo a principal moeda criptografada.

Com o desenvolvimento tecnológico da criptografia, acompanhado do poder da internet, desenvolveu-se um novo sistema de moeda, privado, anônimo e sem qualquer tipo de controle de governos e ou instituições. Esse sistema é o da moeda chamada Bitcoin. Ela pode ser aceita em vários estabelecimentos de comércio e serviços, de forma totalmente anônima, sem quaisquer restrições e taxas financeiras e fronteiriças (HONORATO, 2015).

3.1 Contexto e surgimento

Bitcoin é considerada a primeira “criptomoeda” implementada na história. O conceito de moeda criptografada foi descrito pela primeira vez em 1998 por Wei Dai, apresentando a ideia de uma nova moeda que utiliza criptografia para controlar sua criação e as transações, sem nenhum intermediador financeiro (BITCOIN, 2016).

Já o Bitcoin, propriamente dito, foi introduzido primeiramente em outubro de 2008, quando uma pessoa ou mais sob o pseudônimo de Satoshi Nakamoto publicou o seu artigo, “*Bitcoin: a Peer-to-Peer Electronic Cash System*” em uma lista de discussão *online* de criptografia. Baseado na simples ideia de um “dinheiro eletrônico totalmente descentralizado e *peer-to-peer*, sem a necessidade de um terceiro fiduciário”, o sistema desenhado por Satoshi surgia como um novo experimento no campo financeiro e bancário. A moeda foi batizada Bitcoin, em função do programa de compartilhamento de arquivos *peer-to-peer Bit Torrent*. O projeto vinha a ser uma tentativa de resposta à instabilidade financeira causada pela grande crise financeira do *sub-prime* e também por décadas de monopólio estatal da moeda e por um sistema bancário de reservas fracionárias (ULRICH, 2014).

Não se sabe até hoje a verdadeira identidade de Satoshi Nakamoto, o que frequentemente levantou preocupações sobre o funcionamento e credibilidade do sistema. Entretanto, isso reside no fato da incompreensão da natureza de um programa de “código aberto”. O protocolo e software Bitcoin são públicos e qualquer desenvolvedor pode rever o código ou fazer a sua própria versão modificada do software Bitcoin. Em um sistema de código

aberto qualquer indivíduo pode visualizá-lo e descobrir como se dá seu funcionamento. Qualquer um pode descobrir eventuais falhas no sistema e resolvê-las. Por isso, saber a identidade real de Satoshi não tem grande relevância na prática (BITCOIN, 2016).

De acordo com o Nakamoto (2008), o comércio na Internet veio a depender quase que exclusivamente das instituições financeiras, no papel de intermediários confiáveis, para processar pagamentos eletrônicos. Embora o sistema funcione bem o suficiente para a maioria das transações, ele ainda sofre da fraqueza inerente de um modelo baseado em confiança. O custo da mediação encarece as transações, na prática impondo um valor mínimo aceitável para cada transação, impedindo a existência de transações pequenas e casuais.

Também cita o fato de haver um custo embutido no sistema, já que as transações bancárias tradicionais são reversíveis. Se uma transação pode ser desfeita, aumenta a necessidade de um intermediário confiável. Comerciantes temem seus clientes, requisitando deles mais informações pessoais do que seriam, de outra forma, necessárias. Uma certa taxa de fraude é aceita como inevitável (NAKAMOTO, 2008).

Estes custos e incertezas no pagamento podem ser evitados pelo uso de dinheiro vivo, porém ele implica pagamento presencial. Até o momento do *paper* não existia mecanismo algum para fazer pagamentos através de um canal de comunicações – não sem a figura de um intermediário confiável (NAKAMOTO, 2008).

Exposto esse panorama, somado à maior crise financeira desde a Grande Depressão de 1930, o artigo de Nakamoto realmente foi uma grande revolução e atraiu a atenção de inúmeros entusiastas. Entre eles pode-se citar Ulrich, que em 2014 lançou sua obra “Bitcoin: moeda na era digital” onde explica as propriedades da nova moeda e o porquê de sua importância.

Segundo ele, não se pode deixar de notar o avanço do estado interventor, as medidas sem precedentes e arbitrárias das autoridades monetárias na primeira década dos anos 2000 e a constante perda de privacidade que as pessoas vêm enfrentando na maior parte dos países, tanto desenvolvidos quanto emergentes. Esses fatores podem ser considerados como influentes na criação do Bitcoin (ULRICH, 2014).

Entretanto, apesar dos motivos menos tangíveis para criação do Bitcoin poderem ser apenas intuídos, o que realmente possibilitou sua criação foi a revolução da tecnologia da informação e o uso cada vez mais difundido da Internet. Somente a aliança de duas tecnologias, uma rede descentralizada e a criptografia moderna, podem tornar realidade o que há alguns anos era inimaginável. A crise iniciada em 2008, apenas favoreceu o nascimento da nova modalidade transacional. Assim, seu baixo custo de operação vem sendo um fator favorável ao aumento de sua preferência, por empresários e agentes econômicos em geral.

De acordo com Ulrich (2014), em seu livro “Bitcoin: a moeda na era digital”, desde a crise financeira de setembro de 2008, as autoridades monetárias globais lançaram diversas medidas extremas com intuito de “salvar” a economia mundial. Como exemplo cita: resgate de bancos, seguradoras e montadoras; nacionalização de instituições financeiras; trocas de liquidez entre bancos centrais; monetização de dívida soberana; redução das taxas de juros nominais a zero ou abaixo de zero; e compras maciças de ativos financeiros e hipotecas, quase ilimitadas e sem fim predeterminado, os notórios “afrouxamentos quantitativos” (*quantitative easing*). O intuito do *quantitative easing* é dar liquidez aos bancos e com isso incentivar o crédito.

O Bitcoin poderia ser considerado uma alternativa ao paradigma atual, que pode ser visto como: crescente perda de privacidade financeira; autoridades monetárias centralizadas que abusam do dinheiro isento de qualquer responsabilidade; e bancos cúmplices e coadjuvantes no desregramento monetário (ULRICH, 2014).

Ainda, segundo Ulrich (2014), o atual arranjo monetário ao redor do mundo baseia-se no monopólio da emissão de moeda com leis de curso legal forçado e na grande importância dos bancos centrais, responsáveis por organizar e controlar o meio circulante e o sistema bancário. Em grande parte dos países, a tarefa de emissão de moeda é delegada pelo estado ao próprio Banco Central. As moedas hoje emitidas pelos governos não têm lastro algum, senão a confiança nos governos.

A realidade é que recorrer à impressão de dinheiro é algo que os governos naturalmente fizeram ao longo da história para financiar seus déficits, para custear suas guerras ou para sustentar um estado perdulário incapaz de sobreviver apenas com os impostos cobrados da sociedade. O poder de imprimir dinheiro é tentador demais para não ser usado. (ULRICH, 2014, p.36)

Mas, em uma economia moderna, a oferta de moeda não é composta apenas por cédulas e moedas de metal; os depósitos bancários também fazem parte da oferta monetária, uma vez que desempenham a mesma função que a moeda física. Ainda que não “existam” materialmente, os depósitos constituem parte da oferta monetária total. Assim, quando se emite moeda ou se criam depósitos bancários mediante empréstimos, isto poderá gerar inflação se houver excesso monetário real na economia. Os depósitos bancários se multiplicam por meio de um mecanismo chamado reservas fracionárias. Em suma, significa que os bancos podem guardar nos seus cofres apenas uma fração do dinheiro que foi depositado e emprestar o restante ao público (ULRICH, 2014).

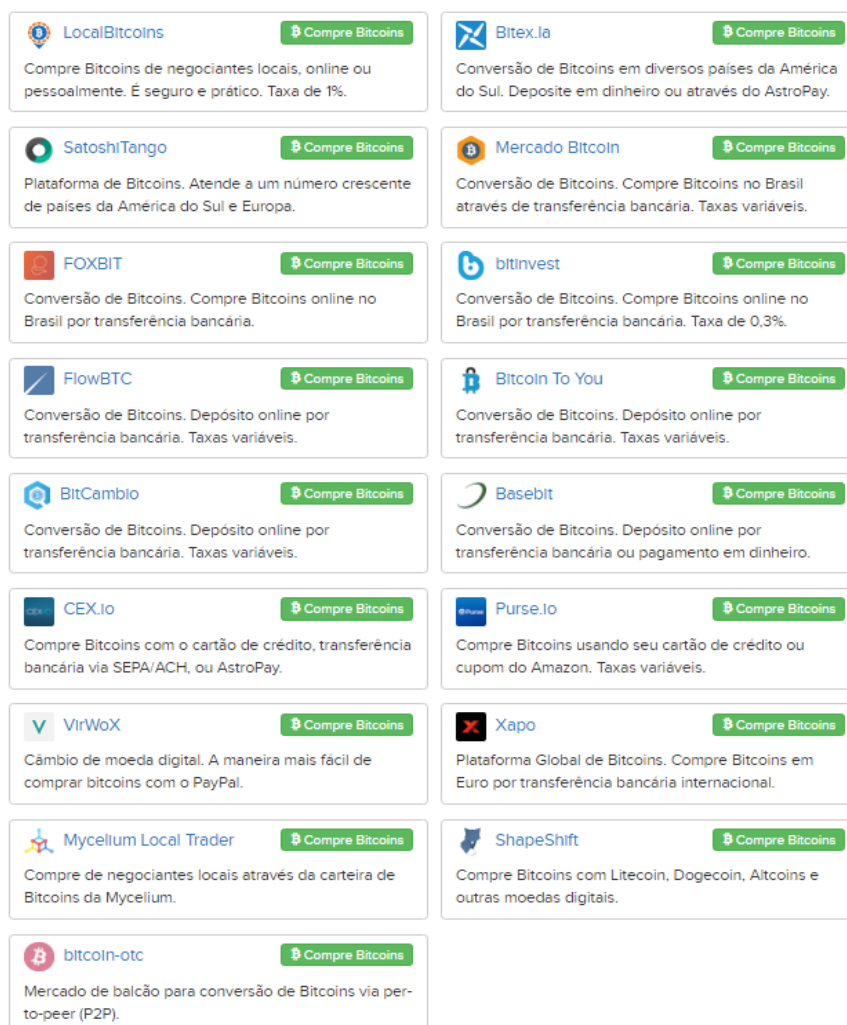
3.2 Funcionamento e características

O Bitcoin é uma moeda digital que pode ser entendido como um protocolo para transações descentralizadas. Isso quer dizer que qualquer pessoa em qualquer lugar do mundo pode fazer uma transferência para qualquer outra pessoa em qualquer outro lugar do mundo sem a presença de um intermediário. É a primeira rede de pagamentos globais descentralizados e baseada em criptografia avançada que aufere à moeda segurança, agilidade e diminuição de custos.

Existem três formas distintas de se obter Bitcoin. A primeira é através da mineração, que será explicada em detalhes posteriormente. A segunda é por meio de casas de câmbio de Bitcoin, onde se pode trocar a moeda convencional por Bitcoin, dada a cotação atual da moeda virtual. A última alternativa é vendendo bens e serviços e aceitando receber a moeda digital em troca.

A forma mais simples de se adquirir Bitcoin é comprando-os em casas de câmbio especializadas. Nesse caso, haverá a troca da moeda tradicional, (real, dólar, euro, etc.) pelo Bitcoin. A criptomoeda é considerada também um ativo financeiro como outro qualquer, com cotação de mercado, rentabilidade e condições de liquidez ou conversibilidade. Na figura 2, podem ser observadas as principais plataformas que brasileiros podem utilizar para adquirir a moeda digital.

Figura 2 - Opções de casas de câmbio para brasileiros comprar e vender Bitcoins



Fonte: BUY BITCOIN WORLD WIDE. Disponível em:
<https://www.buybitcoinworldwide.com/pt-br/brasil/>.

Entretanto, é necessário um lugar para armazenar Bitcoins. Esse local é chamado de *wallet*, que significa carteira em inglês, que funciona basicamente como uma conta em um banco. Após a criação da carteira, o usuário está apto a comprar e vender Bitcoins e a realizar transações com a criptomoeda.

A *wallet* pode ser obtida através de softwares específicos que armazenam os Bitcoins no computador e até mesmo em celulares. Também é possível manter uma carteira online, que normalmente são mais práticas de se usar, porém, se o site for atacado ou a empresa responsável falir, o dinheiro ali depositado será perdido, uma vez que esse mercado não é um mercado

regulado nem possui um agente garantidor dos depósitos. A criação das carteiras não tem nenhum custo, entretanto, alguns sites, como o *Bitgo*, possuem planos com seguro de até 250 mil dólares para usuários norte-americanos.

No caso de manter a carteira no disco rígido de um computador, se ele quebrar ou for roubado, ou ainda caso se perder um *pen drive* ou HD externo contendo Bitcoins ou outras moedas criptografadas, eles também serão todos perdidos. Como medida de segurança é importante manter cópias da carteira em diferentes locais, e sempre criptografadas.

Além de comprar Bitcoins em casa de câmbio ou aceitar receber pagamentos na moeda digital, uma terceira forma de adquiri-los é através da mineração. Esse é processo pelo qual são gerados novos Bitcoins, mas não somente isso, pois é através da mineração que são processados os registros das novas transações de Bitcoin na *blockchain* (uma espécie de livro caixa da rede Bitcoin).

A definição de mineração dada pelo site do Bitcoin no Brasil é a seguinte:

Mineração é o processo de usar capacidade de processamento para processar transações, garantir a segurança da rede, e manter todos participantes do sistema sincronizados. Pode ser considerado como o datacenter do Bitcoin exceto que foi projetado para ser totalmente descentralizado, com mineradores em todos os países e nenhum em particular tendo controle sobre a rede. Este processo é chamado de “mineração” em uma analogia à mineração de ouro porque é um mecanismo temporário utilizado na emissão de novos Bitcoins. Porém diferentemente da mineração de ouro, a mineração de Bitcoin provê uma recompensa em troca dos serviços essenciais para operar uma rede segura de pagamentos. Mineração ainda será necessária depois que o último Bitcoin for emitido.

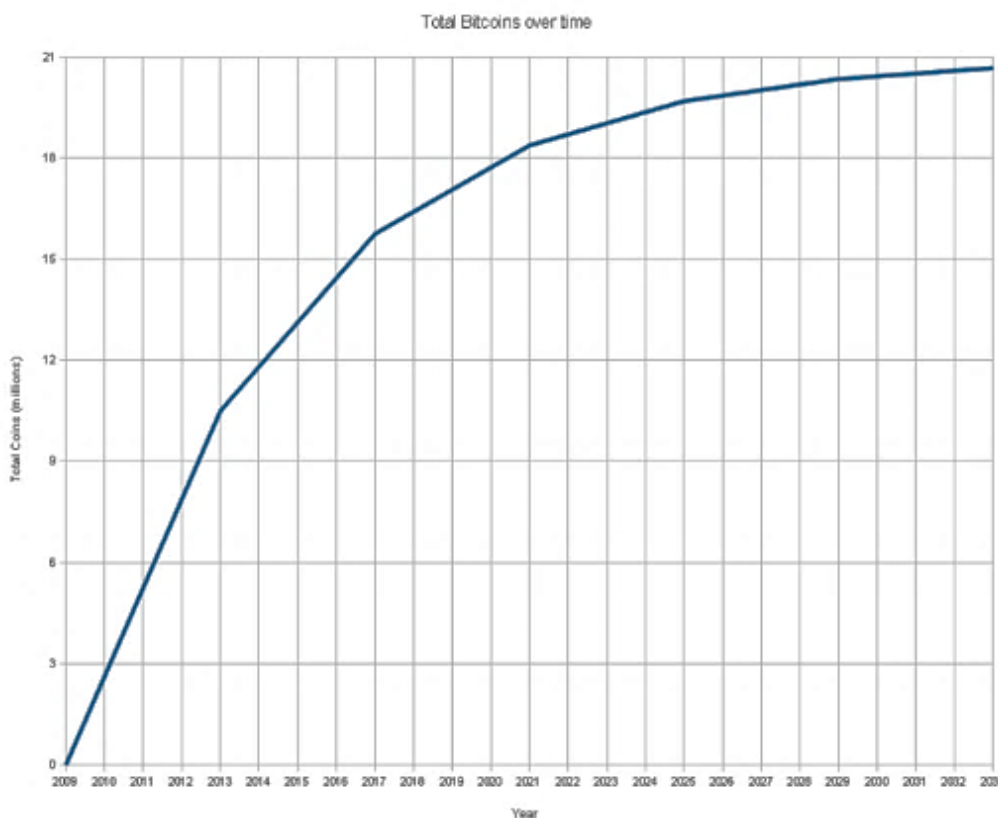
Disponível em: https://bitcoin.org/pt_BR/faq#o-que-e-mineracao-bitcoin.

Todas as transações que ocorrem na rede Bitcoin são lançadas em arquivos chamados de blocos. A moeda é criada (ou “minerada”) quando um novo bloco é adicionado à corrente de blocos prévios. Para isso ocorrer é necessário que os computadores pertencentes à rede realizem cálculos matemáticos complexos, para encontrar um algoritmo que satisfaça as premissas de tornar as transferências irreversíveis e criptografadas. Quem consegue decifrar o código primeiro ganha uma determinada quantidade de Bitcoins, à proporção que a dificuldade desse processo, chamado de “prova de trabalho”, aumenta conforme cresce a capacidade de processamento da rede. Quanto melhor e mais rápido for o computador, mais chances têm de se ganhar Bitcoins (GARCIA, 2014).

Novas unidades de Bitcoins ocorrem quando os blocos são confirmados. Sabe-se de antemão que a taxa de decaimento da criação de moeda é de 50% a cada quatro anos, ou seja, depois desse tempo a recompensa por minerar um bloco cai pela metade. Inicialmente, entre 2009 a 2012, eram pagos 50 BTC por cada bloco “minerado”. De 2012 até 2016 passou para

25. A partir de 09 de julho de 2016 a recompensa atingiu o patamar de 12,5 BTC para todas as vezes que um novo bloco é incorporado a corrente. Como se trata de uma progressão geométrica com infinitos termos, o número limite de Bitcoins em circulação tenderá a ser de BTC 21.000.000, marca prevista a ser atingida em 2140. Em pesquisa realizada no dia 09 de outubro de 2016, a oferta total de Bitcoins era de 15.922.675 BTC, de acordo com dados da *blockchain*. Logo 76% da oferta total de Bitcoins que existirão no futuro já foram gerados. (EUROPEAN CENTRAL BANK, 2012, BRITO & CASTILLO, 2013; BLOCKCHAIN, 2016). O Bitcoin ao ter um limite pré-definido de emissão, se caracteriza mais como um ativo financeiro do que uma moeda, já que seu teto neutraliza seu uso como instrumento de política monetária. Na figura 3, é ilustrada a projeção da oferta de Bitcoins em circulação ao longo do tempo.

Figura 3 - Projeções de unidades monetárias de Bitcoin ao decorrer do tempo



Fonte: Disponível em: https://commons.wikimedia.org/wiki/File:Total_Bitcoins_over_time.png.

Segundo os entusiastas da moeda digital, a limitação da oferta monetária tem como objetivo evitar os processos inflacionários causados pelo aumento excessivo da base monetária.

Entretanto, os críticos do Bitcoin argumentam que o sistema pode ser levado a uma “espiral deflacionária”. Partindo do princípio que o número de usuários aumente expressivamente, e a velocidade da moeda não cresça na mesma proporção, será esperada uma apreciação do Bitcoin, ou seja, uma depreciação dos bens e serviços em relação à moeda digital. Logo, as pessoas teriam um incentivo a guardar seus Bitcoins e não os consumir, acelerando o preço deflacionário (PREVIDI, 2014; EUROPEAN CENTRAL BANK, 2012).

O termo mineração é referência ao fato de haver um dispêndio real – no caso a energia elétrica e o uso de capacidade de processamento do sistema de computadores – e ao limite da oferta, em contraste com as moedas nacionais, em que o Estado e os bancos podem criar moeda a um custo mínimo. Por isso, um dos pontos negativos da mineração de Bitcoins é a necessidade de uma máquina com um potente hardware e o gasto excessivo de energia, pois o computador precisa estar sempre em funcionamento para que seja efetuada a mineração, sendo que, às vezes os gastos com energia ultrapassam a receita ao fim do mês, tornando o processo inviável (GARCIA, 2014).

Com a popularização dos Bitcoins a mineração se tornou algo complicado e competitivo, pois houve um grande aumento do número de usuários minerando e com isso a rede Bitcoin começou a burocratizar a quantidade de moedas geradas, para não inflacionar a moeda. Atualmente, apenas hardwares especializados com ótimo custo-benefício de mineração estão sendo utilizados.

Para se realizar uma transação em Bitcoin, transferência de valores de um endereço para outro, é necessária uma chave privada associada aos endereços. A chave é conhecida somente pelo criador do endereço público, pois somente ele tem o direito sobre seus numerais em valores de Bitcoin. Nesse processo é impossível alguma outra pessoa gastar moedas de outros usuários, já que a criptografia utilizada é de última geração, utilizando métodos comparativos. Seriam necessários milhares de anos nas melhores máquinas existentes para se quebrar uma chave privada de um endereço público, dada à robustez de segurança impregnada no sistema da criptomoeda. (HONORATO, 2015).

A rede da criptomoeda Bitcoin registra todas as transações realizadas, as quais são públicas. Assim as transações ganham transparência e todos possuem o conhecimento do que está acontecendo na rede mundial de computadores. A transparência não anula o anonimato, pois não se sabe quem são os donos dos endereços, apenas que determinado endereço recebeu e colocou determinados valores da criptomoeda à disposição de novas transações (HONORATO, 2015).

Para resolver o problema do gasto duplo, o Bitcoin usa o sistema *blockchain*. Todas as transações são registradas numa espécie de livro-razão público, distribuído e constantemente atualizado, denominado *blockchain*, contendo o histórico de todas as transações realizadas. As novas transações são verificadas contra o *blockchain*, assegurando que os mesmos Bitcoins não tenham sido previamente gastos, evitando o problema do gasto duplo (SILVA, 2015; ULRICH, 2014).

A figura 4 demonstra a exposição de todas as transações de Bitcoins que ocorrem na rede. Nela podem ser vistas as últimas transações que ocorreram no dia 12 de outubro de 2016.

Figura 4 - Últimas transações de Bitcoin expostas na blockchain

Últimas Transações		
0f7cae5e659209be4741cb84e...	< 1 minute	\$ 165.91
2698bbf47193e5fc289fe2c3a...	< 1 minute	\$ 156.86
edca464c840ea815425fcd85c...	< 1 minute	\$ 155.65
fac1af00f5f6bc73920b77e0b...	< 1 minute	\$ 5,777.28
a8ba93978383cda43d8650afc...	< 1 minute	\$ 85.49
4b56128c3bf1c90cd7a25f828...	< 1 minute	\$ 2,090.31
b22da477ec1f101ad0c6754cb...	< 1 minute	\$ 500.84
776361fa81493c6a8fa153b1d...	< 1 minute	\$ 198.38
81e7c818e6b2e2ebb22a5590d...	< 1 minute	\$ 170.60
7e1f660f5af056468f16e107f...	< 1 minute	\$ 5,546.63

Fonte: BLOCKCHAIN. Disponível em: <<https://blockchain.info/pt>>.

Para se realizar uma transação, é necessário que o comprador assine digitalmente com sua chave privada. A transferência será confirmada após o último bloco, com os dados das transferências ocorridas nos últimos 10 minutos, ser incorporado à blockchain. Como cada

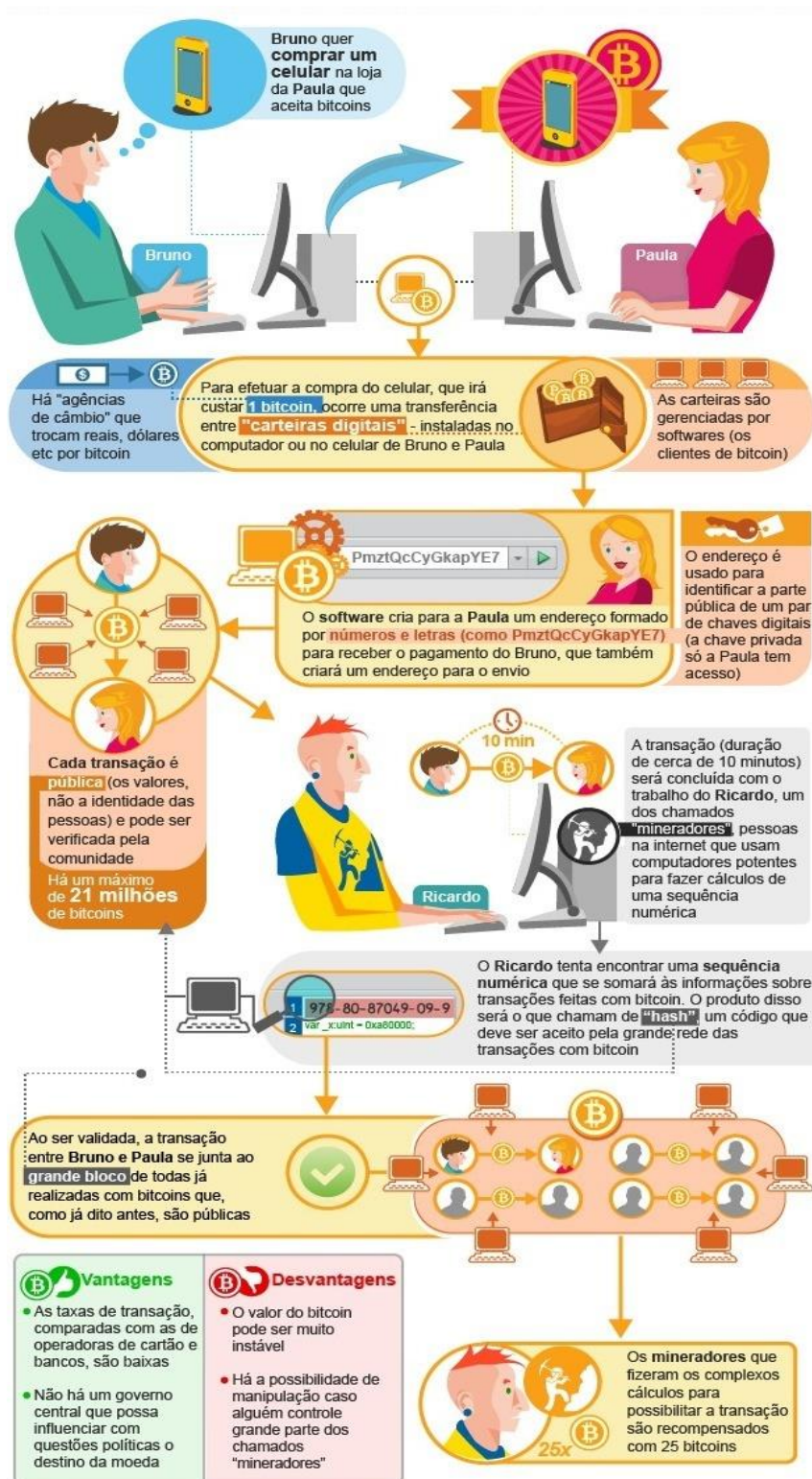
participante da rede possui uma cópia com todos os registros de transações já ocorridos na rede, somente seria possível burlar o sistema se um computador ou rede de computadores tivesse capacidade de processamento maior que a soma de todos os outros, o que é muito improvável (GARCIA, 2014).

A maior parte das transações pode ser processada sem taxas, mas os usuários podem pagar uma pequena taxa voluntária se desejarem uma confirmação mais rápida de suas transações. Quando taxas são necessárias, elas normalmente não excedem alguns centavos (BITCOIN, 2016).

Não há a necessidade do computador estar ligado para receber Bitcoins. Se a transação ocorrer enquanto a máquina do recebedor está desligada, eles aparecerão na próxima vez que o aplicativo da carteira for iniciado. Bitcoins não são realmente recebidos pelo software em um computador, eles são anexados a um registro público que é compartilhado entre todos os dispositivos na rede (BITCOIN, 2016).

O colunista Altieres Rohr, em uma notícia do site G1, simulou através de um infográfico todas as etapas de uma transação de Bitcoins. A figura 5, a seguir, foi editada e demonstra o processo.

Figura 5 - Como funciona uma transação com Bitcoins



























Fonte: Editado pelo autor com base em "Entenda como é uma transação feita com a moeda virtual Bitcoin". Disponível em:
<http://g1.globo.com/tecnologia/noticia/2014/02/entenda-como-e-uma-transacao-feita-com-moeda-virtual-bitcoin.html>

3.3 Outras moedas digitais

Apesar do Bitcoin ser a criptomoeda mais conhecida e realmente concentrar o maior volume financeiro, existem outras moedas digitais que cumprem o mesmo papel do Bitcoin. Na figura 6 podem ser observadas as doze principais moedas criptografadas em 2016.

Figura 6 - Criptomoedas por capitalização de mercado

▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$9,749,350,806	\$612.92	15,906,504 BTC	\$68,793,200	0.51%	
2	 Ethereum	\$1,109,961,049	\$13.11	84,667,804 ETH	\$9,603,370	-1.19%	
3	 Ripple	\$263,640,666	\$0.007432	35,475,196,836 XRP *	\$5,062,610	-6.75%	
4	 Litecoin	\$184,152,876	\$3.85	47,861,254 LTC	\$1,313,350	0.55%	
5	 Ethereum Cla...	\$99,565,745	\$1.18	84,600,004 ETC	\$1,980,010	1.29%	
6	 Monero	\$86,152,977	\$6.60	13,053,600 XMR	\$9,257,930	-13.72%	
7	 Dash	\$81,350,510	\$11.98	6,791,604 DASH	\$449,974	-0.39%	
8	 Steem	\$67,396,251	\$0.410869	164,033,430 STEEM	\$125,896	-0.17%	
9	 NEM	\$38,793,780	\$0.004310	8,999,999,999 XEM *	\$29,431	1.37%	
10	 Dogecoin	\$24,745,648	\$0.000233	106,324,969,492 DOGE	\$80,241	0.75%	
11	 Lisk	\$22,725,000	\$0.227250	100,000,000 LSK *	\$297,170	-3.03%	
12	 Factom	\$22,339,353	\$2.55	8,753,219 FCT *	\$3,158,150	-0.75%	

Fonte: CRYPTO-CURRENCY MARKET CAPITALIZATIONS. Disponível em: <https://coinmarketcap.com/currencies/> (2016).

Como pode ser constatado, o Bitcoin possui enorme participação no mercado das moedas digitais. De acordo com os dados do site *Crypto-currency Market capitalizations* o Bitcoin tem peso relativo de 79,4% do total dessas moedas. Existem atualmente 653 diferentes moedas criptografadas, onde a maioria tem pequena expressão. Em outubro de 2016 esse mercado era de mais 12,2 bilhões de dólares.

4 ANÁLISE DO BITCOIN

Após descrever como se formou o dinheiro e quais são as características básicas de uma moeda, explorar as características e o funcionamento da principal criptomoeda, o Bitcoin, o capítulo em questão terá como foco elucidar o principal objetivo da monografia, qual seja: o Bitcoin é um concorrente ou coopera com a moeda tradicional centralizada em bancos centrais?

4.1 Vantagens e desvantagens do uso do Bitcoin

Existem algumas vantagens que tornaram o Bitcoin motivo de interesse para muitas pessoas. Entre essas vantagens pode-se citar a liberdade de pagamento com essa criptomoeda. É possível enviar e receber qualquer quantia de dinheiro instantaneamente em qualquer lugar do mundo a qualquer momento. Portanto não há feriados nem fronteiras. O Bitcoin permite que seus usuários estejam em pleno controle de seu dinheiro (BITCOIN, 2016).

Outra característica importante é que as taxas são muito baixas. Pagamentos com a criptomoeda são processados tanto sem taxas ou com taxas muito pequenas. Os usuários podem pagar taxas de transações, se desejarem que suas transferências tenham prioridade e possam ser confirmadas mais rapidamente pela rede. Ademais, os comerciantes recebem auxílio de processadores comerciais convertendo Bitcoins em moedas tradicionais e depositando diretamente fundos nas contas bancárias dos comerciantes. Como estes serviços são fundamentados em Bitcoin, eles podem ser ofertados com taxas muito mais baixas do que com *PayPal* ou redes de cartão de crédito (BITCOIN, 2016).

Como não há um terceiro intermediário, as transações de Bitcoin são consideravelmente mais baratas e rápidas do que as feitas por redes de pagamentos tradicionais. O Bitcoin é atrativo a pequenas empresas de margens apertadas que buscam formas de reduzir seus custos de transação. O uso de cartões de crédito trouxe praticidade e agilidade às transações, mas seu uso vem acompanhado de pesados custos aos comerciantes (ULRICH, 2014).

As transações de Bitcoin são seguras, irreversíveis e não contêm informações confidenciais ou pessoais dos clientes. Com isso, os comerciantes ficam protegidos de perdas causadas por fraudes ou estornos fraudulentos, permitindo que eles possam expandir para novos mercados, onde os cartões de crédito não estão disponíveis ou taxas de fraude são muito elevadas. Os resultados são taxas mais baixas, mercados maiores e menos custos administrativos (BITCOIN, 2016).

Uma vantagem relevante da criptomoeda é sua utilização para fins de remessa de dinheiro para o exterior. O Bitcoin permite remessas baratas e instantâneas e a redução de custo dessas remessas aos consumidores pode ser considerável. Muitas pessoas utilizam serviços tradicionais como Western Union ou a Money Gram, que cobram pesadas taxas, além de demorar vários dias para finalizar a transferência dos fundos. No primeiro trimestre de 2013, a taxa média por esses serviços girou em torno de 9%. Já as taxas de transações na rede Bitcoin tendem a ser menos de 1% da transação (ULRICH, 2014).

Para Ulrich, o Bitcoin também pode ser encarado como uma potencial arma contra a pobreza e a opressão. Isso porque pode aumentar o acesso a serviços financeiros básicos em locais mais pobres. Segundo ele, devido às dificuldades de se desenvolver serviços bancários tradicionais em áreas menos desenvolvidas, as pessoas em países em desenvolvimento têm recorrido à rede de telefonia móvel para fazer frente às necessidades financeiras. Como um sistema aberto de pagamentos, o Bitcoin pode fornecer a essas pessoas acesso barato a serviços financeiros, em uma escala global (ULRICH, 2014).

O Bitcoin pode também auxiliar os indivíduos que vivem em países com controles de capitais. A moeda digital pode proporcionar uma válvula de escape para pessoas que desejam uma alternativa à moeda depreciada de seu país ou a mercados de capitais estrangulados. Já há casos de pessoas recorrendo ao Bitcoin para proteger-se dos efeitos nocivos dos controles de capitais e da má gestão de bancos centrais (ULRICH, 2014).

Contudo, um possível aumento do uso de Bitcoins levaria ao decréscimo no uso da moeda soberana, dessa forma seria reduzida sua circulação, prejudicando o alcance das políticas monetárias. A ampla substituição da moeda emitida pelo Banco Central por Bitcoins, ou por qualquer outra moeda virtual privada, poderia reduzir significativamente a influência das autoridades monetárias em controlar as taxas de juros de curto prazo. A própria transmissão das mudanças de juros pelos bancos centrais pela economia, e o controle sobre moeda e crédito, poderiam tornar-se menos efetivos (VAN DER LAAN, 2014).

Os usuários do Bitcoin têm todo o controle de suas transferências, pois os comerciantes são impossibilitados de realizar cobranças indesejadas ou não notificadas, como pode ocorrer com outros meios de pagamento. As transações com Bitcoin podem ser efetuadas sem vincular informações pessoais à operação, oferecendo forte proteção contra furto de identidade. Além disso, as pessoas que utilizam Bitcoin, podem proteger seu dinheiro com cópias de segurança e criptografia (BITCOIN, 2016).

Toda informação em relação à própria moeda Bitcoin está facilmente disponível na *blockchain* para qualquer um verificar e utilizar em tempo real. Nenhuma pessoa ou

organização pode controlar ou manipular o protocolo Bitcoin, porque este é criptograficamente seguro. Isso permite que a rede Bitcoin seja confiável, já que ela é completamente neutra, transparente e previsível (BITCOIN, 2016).

Entretanto há desvantagens e desafios que o Bitcoin e as criptomoeda deve superar para talvez no futuro sejam as principais moedas utilizadas nos mercados.

A moeda criptografada possui pequeno grau de aceitação. Muitas pessoas ainda não têm conhecimento sobre ela. A cada dia, mais empresas aceitam Bitcoins, porque eles visualizam as vantagens de seu uso, mas a lista continua pequena e ainda precisa crescer, para que os benefícios da rede sejam maiores.

A volatilidade é outro problema enfrentado pelo Bitcoin. O valor total do número de Bitcoins em circulação e o número de transações na moeda digital ainda não são expressivos. Portanto, eventos relativamente pequenos podem afetar significativamente o seu preço. Em teoria, esta volatilidade irá diminuir à medida que o mercado e a tecnologia Bitcoin amadureçam (BITCOIN, 2016).

O Software Bitcoin ainda está em desenvolvimento, com muitas funcionalidades incompletas, porém em desenvolvimento ativo. Novas ferramentas, recursos e serviços estão sendo desenvolvidos para fazer o Bitcoin mais seguro e acessível para todos. Grande parte dos negócios com a criptomoeda são recentes e ainda não oferecem a segurança adequada. Pode-se dizer que o Bitcoin ainda está em processo de amadurecimento (BITCOIN, 2016).

Se por acaso ocorrer a perda da carteira, os Bitcoins ficam perdidos para sempre. Não há nenhuma maneira de recuperá-los. Você pode perder sua carteira, se seu celular ou computador for roubado. Mas é possível criar backups de sua carteira em dispositivos externos. Uma vez que o arquivo digital esteja perdido, o dinheiro está perdido, da mesma forma com dinheiro vivo de papel. Se as pessoas não protegem seus endereços Bitcoin, elas podem estar mais sujeitas ao roubo. As carteiras de Bitcoin agora podem ser protegidas por criptografia, mas os usuários devem selecionar a ativação da criptografia (ULRICH, 2014).

As carteiras digitais podem ser hackeadas e Bitcoins podem ser roubados. As casas de câmbio de Bitcoin também enfrentaram complicações de segurança. Em fevereiro de 2014, o então maior intercâmbio do Bitcoin, a empresa MtGox, anunciou que mais de 450 milhões de dólares de Bitcoins estavam faltando e que foram, presumivelmente, roubados. Todos os maiores roubos de moedas têm ocorrido nestes “bancos” de armazenamento de moedas, onde as pessoas mantêm seus Bitcoins até que estejam prontos para gastá-los. Infelizmente, devido à falta de regulamentação dessas instituições, não há meio de certificar os procedimentos de

segurança para o armazenamento e gerenciamento de moedas e contas. Sem regulações e proteções de terceiros, é quase impossível recuperar Bitcoins roubados.

De acordo com reportagem vinculada pela Folha de São Paulo, em agosto de 2016, a moeda virtual sofreu mais um ataque a sua reputação. Uma das maiores plataformas de Bitcoin, a Bitfinex, com sede em Hong Kong, suspendeu suas operações devido ao ataque de hackers. Foram roubados 119.756 Bitcoins das carteiras de seus clientes, uma soma equivalente a US\$ 65 milhões, de acordo com o câmbio do dia. O ataque provocou uma desvalorização imediata de cerca de 20% da criptomoeda.

De acordo com Ulrich, é muito importante o papel do usuário para tornar o Bitcoin seguro:

Obviamente, muitos dos riscos de segurança enfrentados pelo Bitcoin são similares àqueles com os quais moedas tradicionais também se defrontam. Notas de reais podem ser destruídas ou perdidas, informação financeira pessoal pode ser roubada e usada por criminosos e bancos podem ser assaltados ou alvos de ataques DDoS. Os usuários de Bitcoin deveriam aprender sobre e como preparar-se contra riscos de segurança, da mesma forma que o fazem com outras atividades financeiras. (ULRICH, 2014, p.30)

Entretanto, se ocorrer algum problema com os meios de pagamentos tradicionais, a pessoa pode procurar a justiça para defender-se, o que não ocorre com o Bitcoin, já que ele não é regulado por nenhuma autoridade.

As transações altamente anônimas que o Bitcoin oferece podem ser facilmente usadas para transações ilegais, como, por exemplo, a compra de armas, drogas online e como uma forma de lavagem de dinheiro. Assim como o dinheiro vivo, ele pode ser usado tanto para o bem quanto para o mal. O fato de se usar pseudônimo no Bitcoin permite que compradores adquiram produtos ilegais online, da mesma forma que o dinheiro tem sido tradicionalmente usado para facilitar compras ilícitas pessoalmente (ULRICH, 2014).

Em relação à lavagem de dinheiro, levando em consideração as características da rede, o Bitcoin pode ser uma opção para as pessoas que desejam mover dinheiro sujo discretamente. Entretanto, o Bitcoin é uma moeda descentralizada aberta que fornece um registro público de todas as transações. Logo, lavadores de dinheiro podem tentar proteger seus endereços de Bitcoin e suas identidades, mas seus registros de transações serão sempre públicos e acessíveis a qualquer momento pelas autoridades. Em contrapartida, muitas casas de câmbio de Bitcoins têm tomado as medidas necessárias para estar em dia com as regulações e exigências das autoridades no que tange ao combate à lavagem de dinheiro, buscando coletar informações dos

usuários. Isso certamente fará o Bitcoin menos atrativo àqueles que desejam o utilizar como meio de lavagem de dinheiro (ULRICH, 2014).

O Bitcoin e as moedas digitais não são regulados. As normas não se aplicam ao Bitcoin porque não é uma moeda oficial e, dado que as moedas virtuais são relativamente novas, os governos ainda não emitiram regulamentos. Isto significa que não há nenhuma proteção para cobrir eventuais perdas. Fraude e golpes piramidais são frequentes, já que cada vez mais, os golpistas se aproveitam da falta de proteções legais que permeiam o uso desse tipo de moeda. A Autoridade Bancária Europeia advertiu aos consumidores destes riscos. Ao contrário da moeda tradicional, se ocorrer algum problema com o dinheiro do usuário em Bitcoin, o indivíduo não terá como se defender na justiça (NOVAES, 2014).

Outro ponto é que os governos não têm como cobrar impostos sobre a moeda virtual. Isso pode virar um problema num possível futuro onde o uso da moeda virtual rivalizará com o da moeda real, a ponto de prejudicar a arrecadação pública.

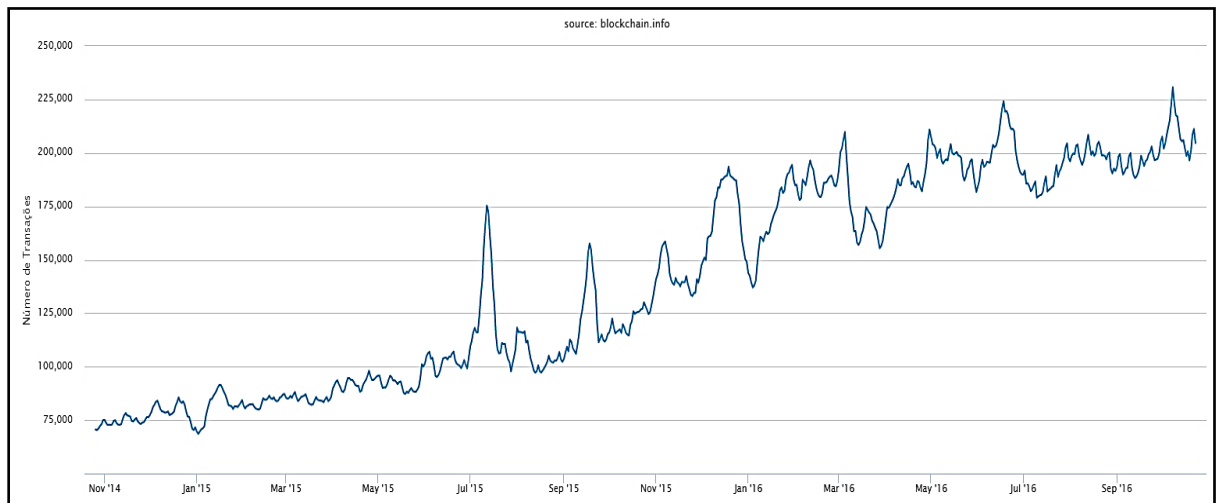
4.2 Análise de dados

O objetivo desta seção é avaliar os dados da moeda digital com o intuito de observar o tamanho deste mercado e qual sua tendência de crescimento. A principal fonte de informação sobre as transações em Bitcoins pode ser encontrada no site da *blockchain*.

A seguir as figuras 7 e 8 representam as médias móveis de sete dias, respectivamente, para o número diário de transações de Bitcoins³ e para o volume de BTCs movimentados diariamente (medido em dólares) nos últimos dois anos. Analisando os dois gráficos fica evidente o aumento do uso da moeda digital como meio de pagamento.

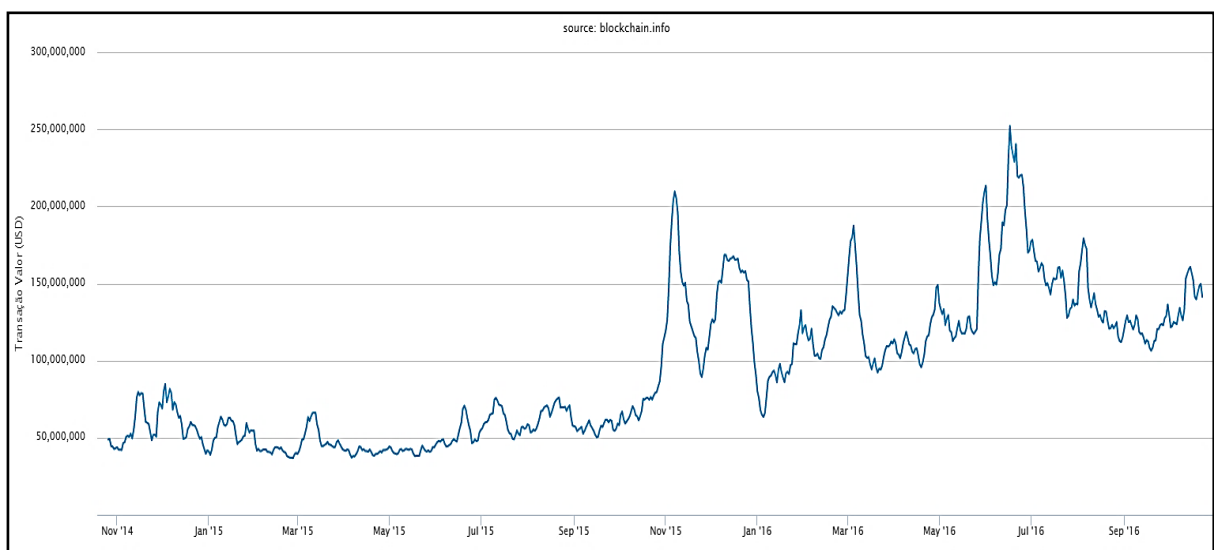
Atualmente ocorrem cerca de 200 mil transferências todos os dias na rede Bitcoin. No fim de 2014 as transações na moeda digital giravam em torno de 75 mil transações/dia. Houve um crescimento de mais de 160% em apenas dois anos. Apesar do aumento expressivo, as transações em Bitcoins ainda representam uma parcela muito pequena das transações financeiras que acontecem ao redor do mundo todos os dias.

³ Excluídos os 100 endereços mais populares.

Figura 7 - Volume de transações em Bitcoins

Fonte: BLOCKCHAIN. Disponível em: <<https://blockchain.info/pt>>.

O volume financeiro das transações em Bitcoin também teve aumento expressivo nos últimos dois anos. No final de 2014 eram transacionados por dia cerca de 50 milhões de dólares em Bitcoin. Já, no final de outubro de 2016, o volume financeiro era de cerca de 140 milhões de dólares, o que configurou em uma alta de 180%. Como se pode observar no gráfico há uma alta volatilidade no volume estimado de transações em USD por dia, entretanto a trajetória de incremento é evidente.

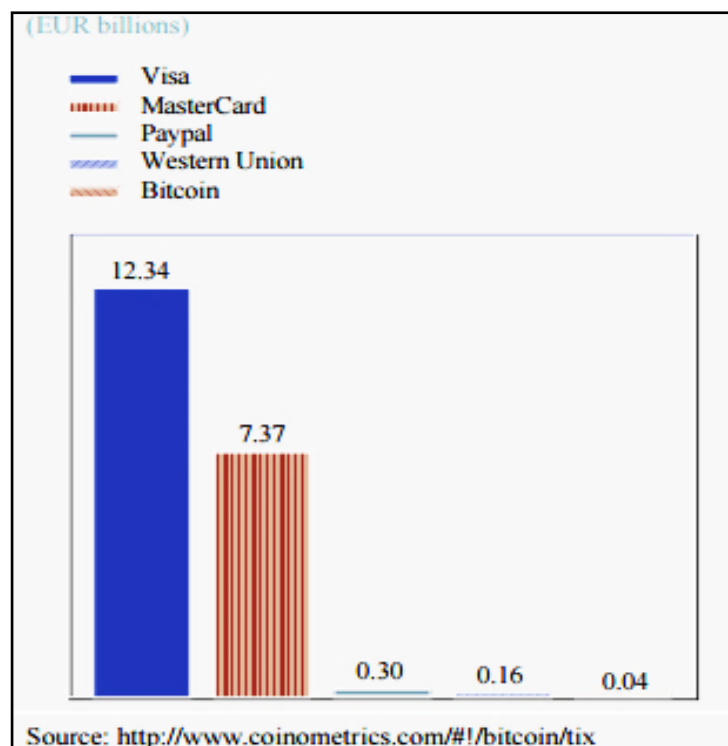
Figura 8 - Volume estimado de transações em USD

Fonte: BLOCKCHAIN. Disponível em: <<https://blockchain.info/pt>>.

As figuras 9 e 10, retirados do relatório do Banco Central Europeu de 2015, demonstram como o Bitcoin, apesar de estar crescendo e aumentando sua participação na economia, ainda representa uma parcela muito pequena do sistema monetário internacional. A figura 9 sinaliza que enquanto em agosto de 2014 Visa e Mastercard transacionavam todos os dias e conjuntamente 19,71 bilhões de dólares, o Bitcoin transacionava apenas 40 milhões de dólares. Logo, a criptomoeda representava apenas 0,2% das transações mundiais realizadas com as soluções de pagamento Visa, Mastercard, Paypal e Wester Union.

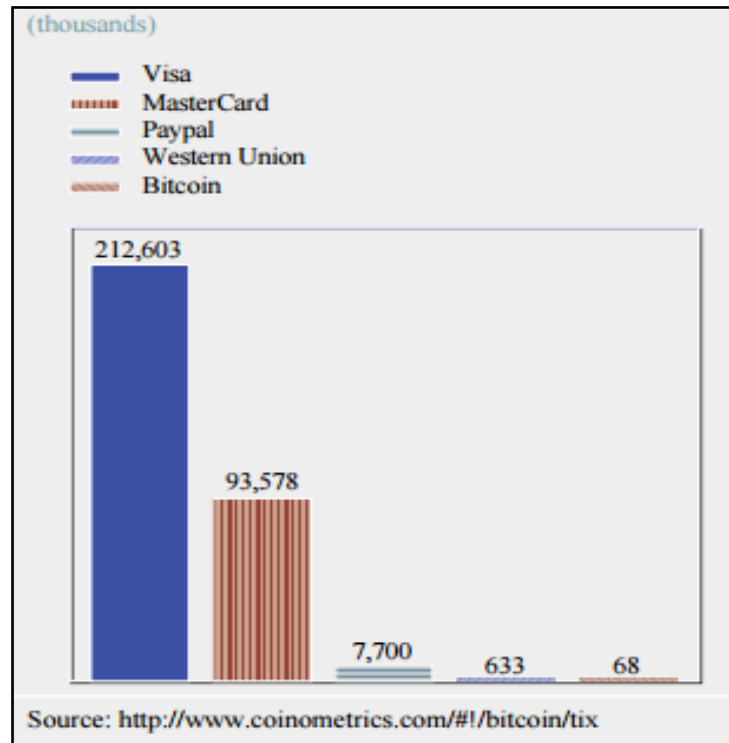
Em relação ao número de transações o panorama não é muito diferente. Em agosto de 2014, o Bitcoin era responsável por apenas 0,02% das transações que ocorriam diariamente no mundo, contando as principais soluções de pagamento eletrônico.

Figura 9 - Volume global de transações diárias com Bitcoin e com as principais soluções de pagamento em agosto de 2014



Fonte: VIRTUAL CURRENCY SCHEMES. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>.

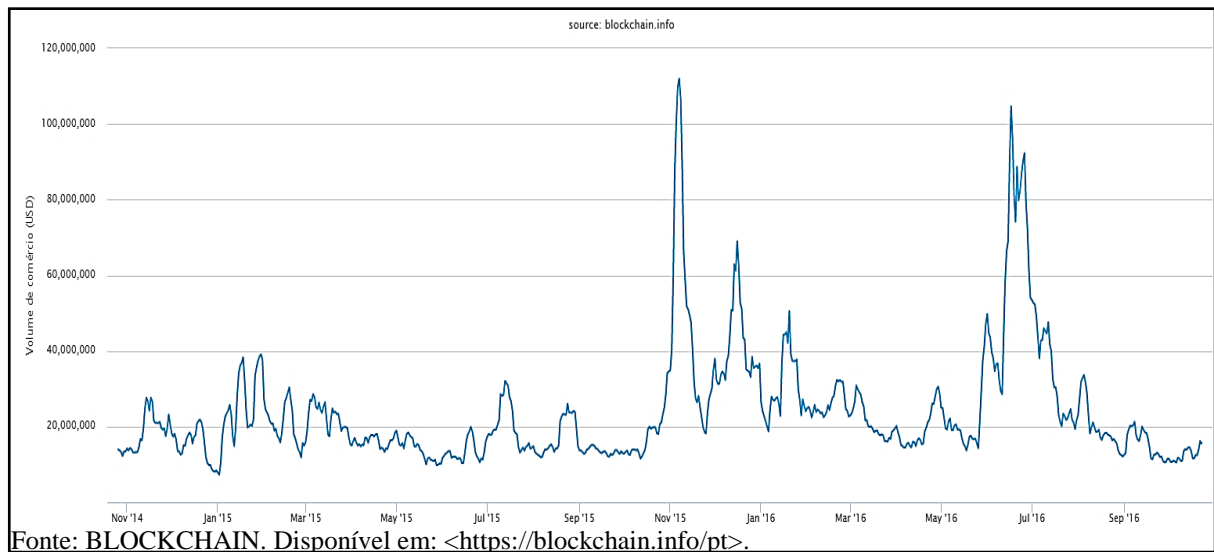
Figura 10 - Número global de transações com Bitcoin e com as principais soluções de pagamento em agosto de 2014



Fonte: VIRTUAL CURRENCY SCHEMES. Disponível em:
 <<https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>>.

Já a figura 11 representa as médias móveis de sete dias do volume de trocas de câmbio em dólares americanos. Apesar de alguns pontos *outliers*⁴, o volume manteve-se basicamente estável durante os últimos dois anos, mais ou menos em 25 milhões de dólares ao dia. Isto pode ser um indicativo do menor uso do Bitcoin como ativo especulativo e da maior utilização do mesmo como meio de pagamento, já que o volume e o número de transações em Bitcoins, como demonstrado anteriormente, cresceu no mesmo período.

⁴ Em estatística, outlier é uma observação que apresenta um grande afastamento das demais da série.

Figura 11 - Volume de trocas de câmbio em USD

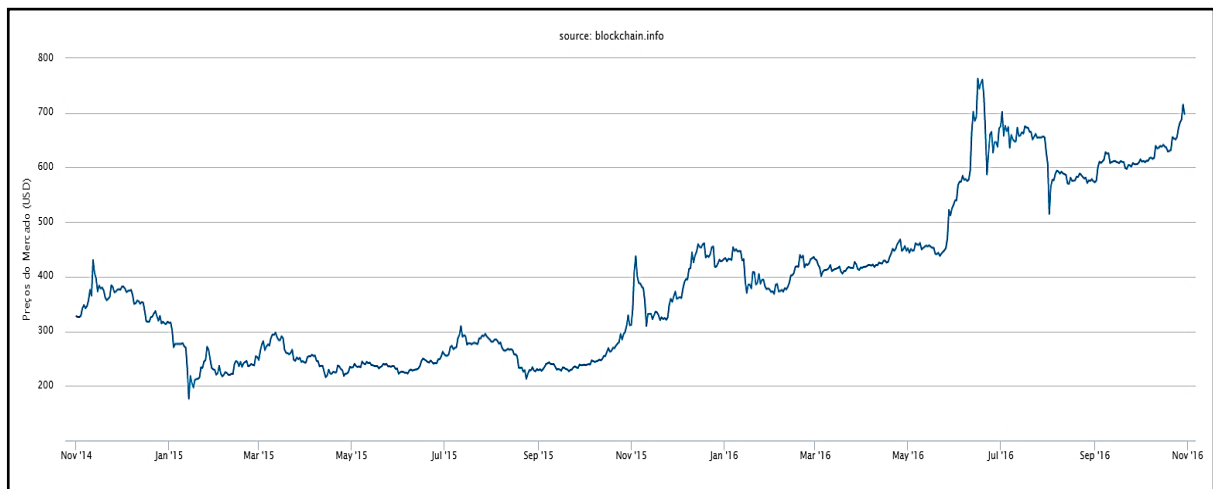
O preço do Bitcoin variou muito desde sua criação. Atualmente, conforme consulta feita no dia 30 de outubro de 2016, uma unidade de Bitcoin era cotada a U\$ 698. Entretanto, no fim de novembro de 2013 o preço da moeda virtual era U\$ 1.084 e em janeiro de 2015 apenas U\$ 212. Apesar de do ano de 2016 o preço ter estabilizado um pouco, a volatilidade ainda é muito expressiva. Enquanto a volatilidade do real frente ao dólar foi de 18,47% nos últimos doze meses, a do Bitcoin em relação ao dólar foi de 37,45%, no mesmo período. O preço do Bitcoin é formado pela interação da oferta e demanda de mercado, logo, está sujeito a especulações, o que o pode tornar instável e imprevisível.

Segundo Ulrich, alguns analistas acreditam que a volatilidade prediz o fim do Bitcoin. Entretanto, para outros, essas flutuações acabam por realizar testes de estresse à moeda e podem, com o passar do tempo, diminuir em frequência conforme mecanismos se desenvolvam. A volatilidade pode ser um grande problema se Bitcoins são usados apenas como reserva de valor ou unidade de conta. Quando a moeda digital é usada como meio de troca, a volatilidade não é um problema tão grande (ULRICH, 2014).

Comerciantes podem precificar seus produtos em termos de moeda tradicional e aceitar o equivalente em Bitcoins. Clientes que adquirem Bitcoins para realizar uma só compra não se importam com o câmbio amanhã; eles somente se preocupam com que o Bitcoin reduza custos de transações no presente. (ULRICH, 2014, p. 29)

A utilidade do Bitcoin como meio de troca poderia explicar por que a moeda tem se tornado popular entre comerciantes, a despeito da volatilidade de seu preço. É possível que o valor de Bitcoins venha a apresentar uma menor volatilidade ao passo que mais pessoas se familiarizam com sua tecnologia e desenvolvam expectativas realistas acerca de seu futuro (ULRICH, 2014).

Figura 12 - Preço de mercado do Bitcoin em USD



Fonte: BLOCKCHAIN. Disponível em: <<https://blockchain.info/pt>>.

Não é tarefa fácil quantificar quantos indivíduos possuem e utilizam Bitcoins. Não se pode usar como parâmetro o número de downloads que foram realizados para baixar uma *wallet*, pois uma pessoa pode ter mais de uma carteira e baixar mais de uma vez em diferentes dispositivos. Também não se pode medir pelo número de endereços, pois muitos indivíduos utilizam endereços distintos a cada transação. Tentar descobrir o número de usuários através dos *polls* públicos também é inviável, pois ninguém pode saber quem realmente utiliza Bitcoins.

A estatística mais relevante sobre o número de usuários, pode ser encontrada, no site *blockchain*. De acordo com o site, em 24 de outubro de 2016 havia mais de 9 milhões carteiras cadastradas. Apesar do número em si não representar necessariamente o número de pessoas que possuem Bitcoins, ele dá uma estimativa do tamanho do mercado.

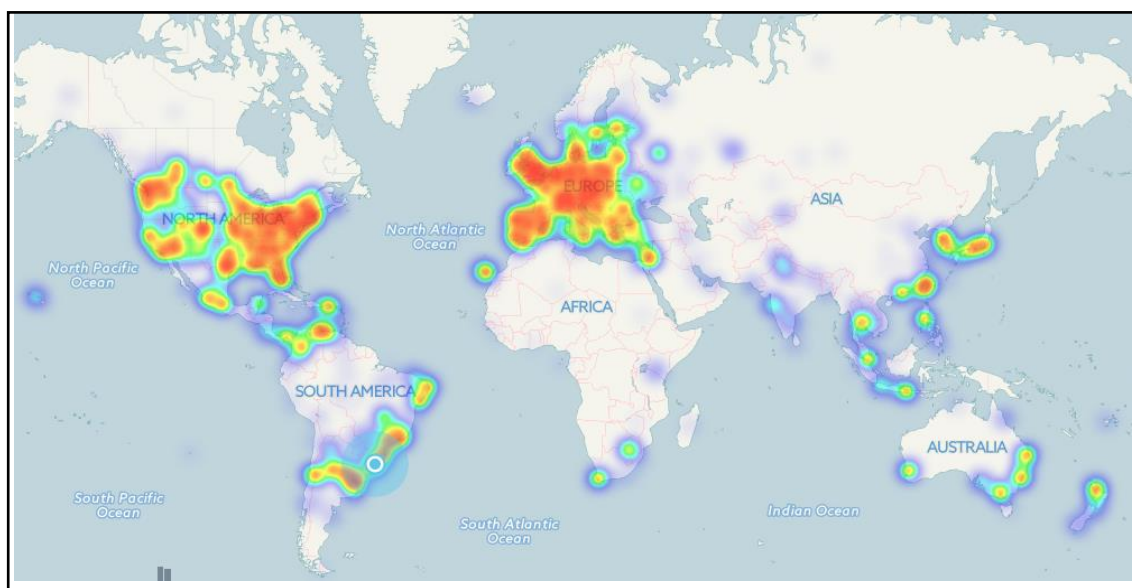
4.3 Aceitação do Bitcoin

Para avaliar se o Bitcoin é um concorrente ou coopera com a moeda tradicional é importante avaliar seu grau de aceitação como moeda e também a sua dimensão relativa. A cada ano aumenta o número de estabelecimentos que aceitam a moeda digital. Devido a sua praticidade e agilidade nas transações é notável o aumento de lojas online e físicas que transacionam com o Bitcoin. Apesar de crescer a cada dia, o número de comerciantes que aceitam receber o pagamento de seus produtos e serviços na moeda digital ainda é pequeno, comparado ao montante global, pois o mercado das moedas criptografadas ainda é incipiente e desconhecido para a grande maioria da população. Portanto, apesar de ser cada vez mais acessível usar o Bitcoin como meio de pagamento, esse ainda é um mercado muito restrito e não é fácil realizar a maioria das transações do dia a dia com ele. A própria representatividade do Bitcoin frente ao agregado monetário M1 ainda é extremamente baixa.

A forma mais prática de encontrar os estabelecimentos é através do site Coinmap⁵, onde estão mapeadas as lojas físicas que aceitam a moeda digital. Segundo esses dados, em 25/10/2016, 8.244 locais aceitavam receber Bitcoins no mundo. Dois anos antes, o número de estabelecimentos era de 5.137. Logo, em dois anos houve um crescimento de 60%. A figura 13, mostra a distribuição desses locais ao redor do globo. Quanto mais próximo do vermelho, maior é a quantidade de estabelecimentos que aceitam a criptomoeda. Fica evidente a concentração nos Estados Unidos e na Europa Ocidental. Entretanto, como a Coinmap não é auditada, ela reflete apenas uma estimativa e deve ser considerada apenas como uma fonte informal de informação.

⁵ COINMAP. Disponível em: <https://en.bitcoin.it/wiki/Trade>.

Figura 13 - Distribuição de estabelecimentos que aceitam Bitcoin ao redor do mundo



Fonte: COINMAP. Disponível em: <<https://coinmap.org/#/world/15.79225357/-41.83593750/2>>.

O site Bitcoin Wiki⁶ traz uma extensa lista, dividida em subcategorias, de comerciantes, sites e empresas que aceitam Bitcoin ao redor do mundo. Há uma grande heterogeneidade dos agentes que operam com a moeda digital.

Dentre os estabelecimentos físicos, pode-se usar Bitcoins para comprar os mais diversos produtos e serviços. É possível usar a criptomoeda em restaurantes, bares, hotéis, pousadas, clínicas médicas, em lojas de roupas e acessórios e até mesmo na área de construção. Algumas grandes empresas internacionais como *Wordexpress*, *Subway*, *Microsoft*, *Reddit*, *Tesla*, *Steam*, *Purse*, *Overstocks*, *Newegg*, *Cheapair*, *Namecheap*, *Tigerdirect*, *Dish Networks*, e *Dell* também aceitam receber seus pagamentos em Bitcoins.

A maioria das empresas que trabalha com Bitcoins já está inserida no mundo virtual. É o caso das empresas de comércio eletrônico, de reserva online (passagens aéreas, hotéis e carros para locação), de produtos eletrônicos (computadores, tablets, softwares diversos, jogos, fones de ouvido, tocadores de música e afins), sites de apostas e serviços de TI (hospedagem de sites e registro de domínio, marketing na internet, web design, desenvolvimento de softwares, segurança de computadores e sistemas).

De acordo com os dados do Coinmap, o Brasil possui 296 locais que trabalham com Bitcoin. O Sudeste é a região brasileira com o maior número de estabelecimentos, 105, destes

⁶ BITCOIN WIKI. Disponível em: <https://en.bitcoin.it/wiki/Trade>.

70 localizam-se no estado de São Paulo. A segunda região com maior quantidade é o Nordeste, onde 56 dos 105 locais pertencem ao estado de Sergipe. A cidade de Aracaju possui uma parte importante dos estabelecimentos que utilizam Bitcoin, porque a cidade recebeu cursos que incentivaram a adoção da moeda por comerciantes e profissionais locais dos mais diversos setores (Quadro 1).

Já a região Sul possui 64 diferentes lugares que aceitam Bitcoins, destes, 29 encontram-se no Rio grande do Sul. Grande parte desses estabelecimentos está ligada ao mundo da informática e a internet, já que o Bitcoin é mais conhecido nesse nicho do que nos outros setores mais tradicionais da economia.

O Brasil possui apenas um caixa eletrônico de Bitcoin que se localiza na cidade de São Paulo. Nele é possível trocar Bitcoins por Reais.

Quadro 1 - Distribuição regional dos estabelecimentos que aceitam Bitcoins no Brasil

Região	Nº
Norte	12
Nordeste	98
Centro-Oeste	17
Sudeste	105
Sul	64
Total	296

Fonte: Elaborado pelo autor, com dados extraídos do site Coinmap. Disponível em: <<https://coinmap.org/#/world/15.79225357/-41.83593750/2>>.

A empresa brasileira Tecnisa, especializada no mercado imobiliário, aceita receber Bitcoins como parte do pagamento. Na verdade, a empresa dá um desconto de 5% para as pessoas que desejarem usar a moeda digital para pagar a entrada de seu imóvel.

4.4 Bitcoin é moeda?

Para responder à questão se o Bitcoin e as moedas digitais são concorrentes ou cooperam com a moeda tradicional, é essencial comparar as características desse tipo de moeda com as tradicionais, para elucidar se elas apresentam os atributos que uma moeda deve ter de acordo com a teoria econômica.

O quadro 2, traz um resumo comparativo dos atributos dos sistemas monetários em ouro, papel-moeda e Bitcoin.

Quadro 2 - Atributos dos sistemas monetários: ouro, papel-moeda e Bitcoin

Atributos	Ouro	Papel-moeda	Bitcoin
1. Durabilidade	Alta	Baixa	Perfeita
2. Divisibilidade	Média	Alta	Perfeita
3. Maleabilidade	Alta	Alta	Incorpóreo
4. Homogeneidade	Média	Alta	Perfeita
5. Oferta (Escassez)	Limitada pela natureza	Ilimitada e controlada politicamente	Limitada matematicamente
6. Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

Fonte: ULRICH, 2014, p. 67.

O Bitcoin satisfaz plenamente o atributo da indestrutibilidade e da inalterabilidade. Como a criptomoeda é intangível e digital, não sofre alteração espacial ou temporal, ao contrário das moedas físicas, como o ouro e o papel-moeda. Os Bitcoins são semelhantes à moeda tradicional quando representada no meio digital – moeda eletrônica (ULRICH, 2014).

Considerando que o Bitcoin circula apenas no meio digital, a sua existência estaria ameaçada caso a internet fosse extinta. Cabe ressaltar que o próprio sistema matemático do Bitcoin e a descentralização não permitiram nenhuma falsificação até o momento (PREVIDI, 2014).

O atributo da homogeneidade é cumprido pelo Bitcoin, já que todas as unidades monetárias são perfeitamente idênticas, já que sua formação é matemática e não física. Outra vantagem é a não dependência de nenhum tipo de medição (PREVIDI, 2014; ULRICH, 2014).

Já em termos da divisibilidade, o Bitcoin é fracionado em oito casas decimais, sendo possível a ampliação da divisão o quanto for necessária, caso o preço de uma fração de Bitcoin atinja valores muito altos (PREVIDI, 2014; ULRICH, 2014). Por isso, apesar do teto da emissão de Bitcoins estar estipulado em 21 milhões de unidades, sua alta divisibilidade a viabilizaria como meio de pagamento mesmo em um cenário de utilização maciça da criptomoeda pelos agentes econômicos.

Em termos de transferibilidade, encontra-se o grande diferencial do sistema, pois as transações têm custo muito baixo e são confirmadas em poucos minutos. Porém, as transferências em Bitcoins encontram o obstáculo da dependência da internet (ULRICH, 2014). Apesar de bem difundida, grande parte da população ainda não tem acesso irrestrito à Internet (PREVIDI, 2014).

O Bitcoin também possui fácil manuseio e transporte, já que são digitais e podem ser armazenados em aparelhos celulares ou em cartões, além dos computadores. Porém, a dependência da internet e a falta de conhecimentos de informática de muitas pessoas pode ser um obstáculo no curto prazo (PREVIDI, 2014; ULRICH, 2014).

Portanto, pode-se afirmar que o Bitcoin satisfaz as principais características exigidas pela teoria econômica.

As principais funções de uma moeda são, como visto no capítulo 2, ser meio de troca, unidade de conta e reserva de valor. Quando a moeda desempenhar satisfatoriamente as três funções, pode-se dizer que alcançou o status de moeda (PREVIDI, 2014; ULRICH, 2014).

Para que um bem exerça a função de meio de troca, basta que seja utilizado como intermediário para trocas indiretas. Para Ulrich (2014, p. 107), o Bitcoin “já atua como um meio de troca, já é uma moeda, embora menos líquida do que as moedas nacionais”. Entretanto, como será exposto posteriormente, não existem muitos locais e comerciantes que aceitam receber Bitcoins em troca de seus bens e serviços. O uso das criptomoedas, no geral, ainda é muito restrito e está longe da liquidez das moedas nacionais. Logo, é possível afirmar que o Bitcoin é um meio de troca, porém limitado a um grupo específico de usuários (PREVIDI, 2014).

O Bitcoin pode servir como reserva de valor, pois muitos usuários as compram como investimento, com a esperança de valorização futura. Grande parte das pessoas que compra Bitcoins não a utiliza como meio de pagamento e sim possuem a expectativa que sua cotação irá aumentar e assim auferirão lucros. Nesse sentido, o Bitcoin pode ser visto como um ativo financeiro.

Entretanto, a cotação da moeda virtual sofre fortes variações constantemente, seu preço possui uma alta volatilidade. Além disso, não possui a mesma liquidez das moedas tradicionais. Por isso, apesar de apresentar a função reserva de valor, não permite que ela seja um ativo seguro para preservação de riqueza. Conforme Ulrich (2014, p. 29): “não faz sentido gerir as finanças de um negócio ou guardar as economias em Bitcoins se o preço de mercado oscila desenfreada e imprevisivelmente” (PREVIDI, 2014).

A instabilidade do preço dos Bitcoins faz com que, dificilmente, os indivíduos a utilizem como unidade de conta. As empresas que aceitam Bitcoins como forma de pagamento precificam os bens em moeda corrente (dólar, real, etc.) para, então, cobrar o equivalente em Bitcoin (VAN DER LAAN, 2014).

Para Van Der Laan, em seu artigo “É crível uma economia monetária baseada em Bitcoins?”, a função monetária básica de unidade de conta parece não existir ainda (até por sua baixa disseminação), pois se trata muito mais de um sistema de pagamento virtual do que propriamente de uma nova moeda com as três funções clássicas. Para ele, a modalidade de moeda criptografada parece, hoje, muito mais apenas um meio de transferir recursos, mas ainda calculados com base nas moedas nacionais correntes. Sua pequena disseminação não permite formação de preços em Bitcoins na economia real. As bruscas oscilações de conversão nas moedas tradicionais impedem basicamente constituir parâmetros para os usuários avaliarem se está caro ou barato um bem ou serviço referenciado naquela moeda (VAN DER LAAN, 2014).

Na visão do *Bank of England*, as moedas virtuais são relativamente pouco usadas. Apesar da alta volatilidade, ela exerce o papel de reserva de valor. Todavia, não são usadas tipicamente como meio de troca e não satisfazem a função unidade de conta. Para o banco citado, o Bitcoin pode ser considerado uma *commodity* digital. Teoricamente, ele pode servir como dinheiro para qualquer pessoa com um dispositivo de acesso à internet, porém, atualmente, como poucas pessoas utilizam o Bitcoin, ele cumpre as três funções da moeda para algumas poucas pessoas (PREVIDI, 2014; ALI *et al.*, 2014).

Pode-se concluir que o Bitcoin possui as características essenciais de uma moeda, entretanto não cumpre plenamente as funções de uma. Ele pode ser considerado como reserva de valor, mas, atualmente, é apenas meio de troca para um limitado grupo de pessoas que

participam da rede. A função unidade de conta também não está hoje em dia presente na moeda digital.

4.5 Regulação

O Bitcoin não é regulado diretamente por nenhum órgão governamental ao redor do mundo. Por ainda representar uma pequena fração das transações financeiras do mundo e seu estoque monetário em dólares ser incomparável a oferta monetária mundial, o Bitcoin e as moedas criptografadas no geral, atualmente, não apresentam risco sistêmico ao funcionamento do mercado financeiro.

Entretanto, as criptomoedas, e em especial o Bitcoin, não estão passando despercebidos aos olhos das autoridades mundiais. Com o crescimento de seu uso, os governos têm demonstrado preocupação quanto aos efeitos das moedas digitais nas áreas de sistemas de pagamento, estabilidade financeira, política monetária e estabilidade dos preços, assim, emitiram notas e pareceres que recomendam aos cidadãos que não utilizem o Bitcoin – ou as moedas virtuais em geral. Apesar disso, as autoridades monetárias não consideram o sistema uma ameaça à estabilidade dos sistemas monetários, apenas um risco aos usuários (PREVIDI, 2014; EUROPEAN CENTRAL BANK, 2012).

O relatório anual disponibilizado pelo *Financial Stability Oversight Council* (FSOC)⁷ em 2016, destaca os receios sobre as moedas digitais. Segundo ele, a tecnologia da *blockchain*, empregada no Bitcoin, é uma das inovações tecnológicas mais importantes nos últimos anos, pois permite que os próprios participantes do mercado façam a gestão de muitos tipos de transação sem a participação direta de terceiros de confiança. Entretanto, representam incertezas e riscos que participantes e reguladores do mercado devem monitorar (FSOC, 2016).

⁷ FSOC (*Financial Stability Oversight Council*/ Conselho de Supervisão de Estabilidade Financeira), inclui o Federal Reserve (Banco Central dos EUA), a Securities and Exchange Commission (Comissão de Valores Mobiliários) e o Departamento do Tesouro. O conselho é encarregado de identificar riscos à estabilidade financeira dos Estados Unidos, promover disciplina no mercado e responder a riscos emergentes à estabilidade do sistema financeiro.

O FSOC observou que o Bitcoin tem presenciado aumentos em falhas de transação e atrasos em algumas negociações. Os atrasos ocorreram devido à velocidade com a qual novas transações superaram a velocidade com a qual elas foram adicionadas ao *blockchain*. O relatório também diz que os reguladores têm que se adaptar à dinâmica estrutura do mercado se eventualmente os sistemas de criptomoeda limitarem a importância dos tradicionais intermediários centralizados. Como as transações em moedas digitais são capazes de ultrapassar fronteiras nacionais ou jurisdições regulatórias, pode ser necessário um “grau considerável” de coordenação entre reguladores para enfrentar e identificar riscos ligados a tais sistemas, de acordo com o relatório (FSOC, 2016).

No dia 24 de novembro de 2015, ocorreu em São Paulo o 1º Seminário de Moedas Digitais da Fundação Getúlio Vargas (FGV). Esteve presente no evento o chefe-adjunto do departamento de supervisão bancária do BACEN, Fábio Lacerda Carneiro. Segundo ele, o Banco Central do Brasil está seguindo de perto as evoluções da tecnologia do protocolo Bitcoin no país, mas a entidade ainda não vê a necessidade de criar uma regulação específica para a moeda digital ou para as *exchanges* brasileiras, já que o tamanho do mercado e o estágio atual de desenvolvimento da tecnologia ainda não justificam a formatação de um arcabouço legal.

O BACEN aprova o fato de que as transações de compra e venda de Bitcoins realizadas por meios das *exchanges* brasileiras possam ser rastreadas, uma vez em que elas se comprometem com a coleta de documentos pessoais das pessoas que acessam suas plataformas, auxiliando em uma eventual necessidade do banco de precisar rastrear transações que possam ser suspeitas de ilegalidade. O próprio Banco Central ainda não tem uma posição definitiva em caracterizar o Bitcoin como moeda, ativo financeiro ou commodity. Os Bancos Centrais dos Países Baixos e da França também alertaram que a moeda não tem garantias governamentais.

Os Bitcoins não são considerados moedas ou valores mobiliários pela regulação brasileira. Entretanto, a Receita Federal os equipara, para fins tributários, aos ativos financeiros, logo estão sujeitos à cobrança do imposto de renda. Os contribuintes foram orientados a declará-las no imposto de renda como “outros bens” quando possuírem mais de R\$1.000,00.

Segundo a Receita Federal, quando as vendas em um mês são maiores que R\$ 35 mil, os ganhos de capital devem ser tributados em 15% e o pagamento do imposto deve feito até o último dia útil do mês seguinte ao da transação. O uso de Bitcoins para compras na internet ou como investimento são atividades lícitas e, seguindo as orientações do fisco, o contribuinte fica protegido de problemas futuros com a receita.

Em 2015, o Deputado Federal Aureo Lidio Moreira Ribeiro do SD-RJ, apresentou o Projeto de Lei nº 2.303/2015, que visa, se aprovado⁸, disciplinar pelo Banco Central e fiscalizar pelo Conselho de Controle de Atividades Financeiras (COAF), as moedas virtuais (como os Bitcoins) e os programas de milhagem das companhias aéreas.

Segundo Aureo Lidio Moreira Ribeiro, em certa medida tanto o Banco Central como o Conselho de Controle de Atividades Financeiras (COAF) e os órgãos do consumidor já têm competência para fiscalizar e regular moedas virtuais. No entanto, entende que as legislações que conferem tais atribuições podem ser mais transparentes em relação a tais atribuições, o que evita desnecessários questionamentos judiciais (Projeto de Lei nº 2.303, 2015)

Em notícia vinculada pelo site da câmara dos deputados⁹, o deputado explica que o objetivo do projeto é dar amparo legal para a criação de um arcabouço regulamentar para o mercado de moedas virtuais. O deputado explicou que os programas de milhagem foram incluídos na proposta porque, segundo entendimento do Banco Central Europeu (BCE), é um tipo específico de moeda virtual. O deputado afirmou que a aprovação do projeto pode “reduzir os riscos das moedas virtuais contra a estabilidade financeira da economia, diminuir a possibilidade de elas financiarem atividades ilegais, além de proteger o consumidor contra eventuais abusos”.

Dado seu restrito alcance atual, sobretudo no Brasil, não se vislumbra risco sistêmico para o funcionamento da economia doméstica ou mesmo para a poupança popular. Constitui, atualmente, assunto muito mais relacionado a preocupações com lavagem de dinheiro e a atividades ilícitas internacionais (VAN DER LAAN, 2014).

⁸ Até o momento que o trabalho foi finalizado, o Projeto de Lei nº 2.303/2015 ainda tramitava no Congresso Nacional.

⁹ Câmara dos Deputados. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/preview-496935.html?timestamp=1443204141838>>.

5 CONCLUSÃO

O presente trabalho buscou explorar o funcionamento de uma criptomoeda, focando-se na principal delas, o Bitcoin. O objetivo geral do estudo era discutir a possibilidade do Bitcoin ser uma moeda concorrente ou cooperar com a moeda tradicional.

Os motivos que deram origem à monografia foram o aumento das transações em Bitcoin, o aumento da aceitação dele como meio de pagamento pelos agentes econômicos e sua alta capitalização de mercado, 11,8 bilhões de dólares em 01 de novembro de 2016.¹⁰ Como esse é um assunto novo, ainda há poucos trabalhos que busquem analisar os impactos de uma moeda digital na economia.

Para isso, discutiu-se no primeiro capítulo o funcionamento geral das moedas tradicionais, bem como sua evolução e principais características. O segundo tratou dos conceitos que envolvem o protocolo Bitcoin. O capítulo posterior buscou analisar as principais vantagens e desvantagens do uso do Bitcoin, assim como explorar sua aceitação, questões referentes à regulação e se o Bitcoin pode ser considerado moeda.

O Bitcoin preenche, de acordo com teoria econômica, as principais características de uma moeda. Ele satisfaz o atributo da indestrutibilidade e da inalterabilidade, já que é intangível e virtual. O Bitcoin também é altamente divisível, pois pode ser fracionado até a oitava casa decimal. Também é homogêneo e possui alta facilidade para transferência, manuseio e transporte.

Entretanto, o Bitcoin não exerce plenamente as três funções principais de uma moeda. Como sua aceitação é ainda muita baixa, possui valor de troca apenas para um limitado grupo de pessoas que transacionam com a moeda. Embora seja notável o aumento das transações em Bitcoins e o número de empresas e agentes que aceitam transacionar com a moeda digital.

A função unidade de conta quase não existe, uma vez em que o valor do Bitcoin ainda oscila muito. As empresas que aceitam Bitcoins como forma de pagamento precificam os bens em moeda tradicional para, então, cobrar o equivalente em Bitcoin. Apesar da volatilidade, o Bitcoin até pode servir como reserva de valor, na medida em que muitos usuários não a utilizam como meio de pagamento e sim como uma forma de investimento e guardar riqueza. Todavia a liquidez do Bitcoin é muito menor do que a das moedas tradicionais.

¹⁰ Fonte: <https://blockchain.info/pt/charts/market-cap>

Como foi exposto, as principais vantagens do Bitcoin que o fizeram ser cada vez mais noticiado pela mídia e utilizado pelos agentes econômicos, é a facilidade, agilidade e baixo custo para realizar transações. Como não há um terceiro intermediário, as transações de Bitcoin são consideravelmente mais baratas e rápidas do que as feitas por redes de pagamentos tradicionais.

Outras vantagens que foram citadas ao longo do trabalho é que transações de Bitcoin são seguras, irreversíveis e não contêm informações confidenciais ou pessoais dos clientes. Também a moeda digital é muito eficiente para realizar remessas ao exterior, já que as transações ocorrem muito mais rápidas e com um preço muito menor. O fato de todas as transações em Bitcoin estarem disponíveis na *blockchain*, torna a rede descentralizada, transparente e neutra. Nenhum indivíduo ou organização pode controlar ou manipular o protocolo Bitcoin, porque este é criptograficamente seguro.

Entretanto nem só de pontos positivos vive o Bitcoin. A moeda digital apresenta alguns pontos negativos importantes que são um grande desafio para o Bitcoin e as moedas criptografadas, no geral se tornarem de fato concorrentes da moeda tradicional.

Apesar de o número de empresas e estabelecimentos que aceitam pagamentos em Bitcoins estar aumentando, o grau de aceitação da criptomoeda ainda é extremamente baixo. A grande maioria da população ainda não tem conhecimento sobre ela. Ela está muito mais ligada ao mundo digital e as pessoas que o conhecem.

A volatilidade ainda é um problema enfrentado pelo Bitcoin. A cotação da criptomoeda varia muito. Isso pode ser um fator que assusta indivíduos e empresas e os previnem de usar o Bitcoin. Outro ponto negativo é que como as transações em Bitcoin são anônimas, elas podem ser utilizadas para atividades ilícitas e como uma forma de lavagem de dinheiro.

Observou-se também que o Bitcoin não é regulado pelas autoridades monetárias dos principais países. Logo, as normas não se aplicam às moedas digitais. Isto significa que não há nenhuma proteção em caso de fraude ou roubo. Como foi exposto no trabalho, os Bitcoins podem ser roubados. Algumas casas de câmbio que funcionam também como bancos para armazenar as criptomoedas, já foram alvos de hackers e perderam milhões de seus clientes. Sem regulações e proteções, é quase impossível recuperar Bitcoins roubados. A maioria dos bancos centrais está apenas monitorando as moedas digitais, uma vez em que não se vislumbra risco sistêmico para o funcionamento da economia devido à pouca expressão das transações nessas moedas.

Analisando todos os aspectos apontados anteriormente, conclui-se que o Bitcoin deve ser visto como um meio de pagamento alternativo, ou seja, uma opção adicional para se realizar transações pela internet. Nesse sentido, o Bitcoin é e será uma moeda que cooperará com a moeda tradicional, pelo menos no curto e médio prazo. Atualmente, o Bitcoin é uma moeda digital de pouco alcance e funciona paralelamente às moedas tradicionais de cunho forçado.

O Bitcoin não deve ser encarado como um concorrente às moedas tradicionais, pelo menos não em um futuro próximo. Como possui baixa aceitação, não possui grande credibilidade e não é garantida por autoridades monetárias, sendo livre de responsabilidade legal, é difícil acreditar que o Bitcoin substituirá ou concorrerá com as moedas soberanas. Também nada garante que não surja nos próximos anos uma moeda virtual com maior vantagem tecnológica que possa substituir o Bitcoin.

Independentemente do sucesso ou fracasso do Bitcoin, a plataforma tecnológica em que ele é baseado, o *blockchain*, muito provavelmente terá implicações mais significativas já no curto prazo. Como foi noticiado na revista *The Economist* de 31 de outubro de 2015, o *blockchain* é uma máquina de confiança, visto que permite que pessoas que não têm nenhuma confiança entre si, possam colaborar sem ter que passar por uma autoridade central. Seu uso vai muito além das moedas criptografadas, pois pode servir de base para garantir a confiança de diversos outros sistemas de troca de informações.

Portanto, é inegável que o Bitcoin possui vantagens não desprezíveis e pode ser utilizado como um meio de pagamento inovador e eficiente. Como é uma tecnologia muito recente, seu verdadeiro potencial ainda está por ser visto. Apesar das autoridades estarem apenas acompanhando seu desenvolvimento, será a disseminação e o alcance de seu uso que determinará o potencial de concorrência com os meios de pagamentos tradicionais.

6 REFERÊNCIAS

- ALI, R. *et al.* **Innovations in payment technologies and the emergence of digital currencies.** Quarterly Bulletin, Bank of England, London, v. 54 n. 3, 2014. Disponível em: <<http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3.pdf>>. Acesso em: 06 nov. 2016.
- BANCO CENTRAL DO BRASIL (BACEN). **BC esclarece sobre os riscos decorrentes da aquisição das chamadas “moedas virtuais” ou “moedas criptografadas”.** Brasília, 2014. Disponível em: <<https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>>. Acesso em: 13 nov. 2016.
- BITCOIN. Disponível em: https://bitcoin.org/pt_BR/>. Acesso em: 6 nov. 2016
- BLOCKCHAIN.INFO. [S.l.], 2014. Disponível em: <<https://blockchain.info/pt/>>. Acesso em: 06 nov. 2016.
- BRITO, J.; CASTILLO, A. **Bitcoin: A primer for policymakers.** Policy: MercatusCenter at George Mason University, Arlington, v. 29, n. 4, p.3-12, 2013. Disponível em: <<http://bestbitcoin.com.br/bitcoin-manual-basico-para-legisladores-e-politicos/>>. Acesso em: 06 nov. 2016.
- BUY BITCOIN WORLDWIDE. Disponível em: <<https://www.buybitcoinworldwide.com/pt-br/brasil/>>. Acesso em: 06 nov. 2016.
- CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.303/2015.** Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1358969&file name=PL+2303/2015>. Acesso em: 6 nov. 2016.
- COINMAP. Disponível em: <<https://coinmap.org/>>. Acesso em: 06 nov. 2016
- CRYPTO-CURRENCY MARKET CAPITALIZATIONS. [S.l.], 2014. Disponível em: <<http://coinmarketcap.com/all/views/all/>>. Acesso em: 06 nov. 2016.
- EUROPEAN CENTRAL BANK – ECB (2012). **Virtual Currency Schemes.** Oct, 2012. Disponível em: <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Acesso em: 08 mai. 2016.
- EUROPEAN CENTRAL BANK – ECB (2015). **Virtual Currency Schemes.** Fev, 2015. Disponível em: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> Acesso em: 09 nov. 2016.
- FELIX, S. **Banco Central: estamos acompanhando a evolução do Bitcoin.** 2015. Disponível em: <https://www.coinbr.net/blog/banco-central-estamos-acompanhando-a-evolucao-do-bitcoin/>. Acesso em: 15 nov. 2016

FINANCIAL STABILITY OVERSIGHT COUNCIL – FSOC. **Anual Report**, 2016. Disponível em: <<https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC%202016%20Annual%20Report.pdf>>. Acesso em: 06 nov. 2016

FOLHA DE S. PAULO. **Bolsa que negocia Bitcoin suspende operações após ataque de hackers**. Agosto 2016. Disponível em: <<http://www1.folha.uol.com.br/mercado/2016/08/1798366-bolsa-que-negocia-bitcoin-suspende-operacoes-apos-ataque-de-hackers.shtml>>. Acesso em: 28 nov. 2016.

GARCIA, R.S. **Moedas virtuais são moedas?** Um estudo de caso para o Bitcoin e o Litecoin. 2014. Trabalho de conclusão (Graduação em Ciências Econômicas) – Faculdade de Ciências Econômicas, Universidade Estadual de Campinas, Campinas, 2014.

HARARI, Y.N. **Sapiens**: Uma breve história da humanidade. 6 ed. Porto Alegre: L&PM, 2015.

HONORATO, Y. A criptomoeda Bitcoin: Cooperação ou concorrente da moeda oficial dos países. In: **VI Congresso Internacional de História**, 2015. Disponível em: <http://www.cih.uem.br/anais/2015/trabalhos/1543.pdf>. Acesso em: 08 mai. 2016.

LOPES, J.C.; ROSSETTI, J.P. **Economia monetária**. 7. ed. São Paulo: Atlas, 1998. 300 p.

MONTORO FILHO, A.F.; TROSTER, R.L. Introdução à teoria monetária. In: PINHO, D.B.; VASCONCELLOS, M.A.S.; TONETO JR., Rudinei(Org.). **Manual de Economia**. Cap. 16, 5 ed. São Paulo: Saraiva, 2004.

NAKAMOTO, S. **Bitcoin**: A Peer-to-Peer Electronic Cash System, 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 08 mai. 2016.

NOVAES, R. **Conheça as vantagens e desvantagens do uso de Bitcoins**. Agosto 2014. Disponível em: <<http://www.psafec.com/blog/bitcoin-amigo-ou-inimigo/>>. Acesso em 28 nov. 2016.

PORTAL DA CÂMARA DOS DEPUTADOS. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/preview496935.html?timestamp=1443204141838>>. Acesso em: 06 nov. 2016.

PREVIDI, G.S. **Descentralização Monetária**: um estudo sobre o Bitcoin. 2014. Trabalho de conclusão (Graduação em Ciências Econômicas) – Faculdade de Ciências Econômicas, Universidade Federal Do Rio Grande do Sul, Porto Alegre, 2014.

ROHR, Altieres. **Entenda como é uma transação feita com a moeda virtual Bitcoin**. 2014. Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/02/entenda-como-e-uma-transacao-feita-com-moeda-virtual-bitcoin.html>. Acesso em: 15 nov. 2016

SILVA, D.E. **Aspectos de segurança na rede Bitcoin**. Disponível em: <http://www.cdn.ueg.br/source/observatorio_inhumas/conteudoN/3322/CAP_8__CR_ASPECTOS_DE_SEGURANCA_NA_REDE_BITCOIN.pdf.pdf>. Acesso em: 06 nov. 2016.

ŠURDA, P. **Economics of Bitcoin**: Is Bitcoin an alternative to fiat currencies and gold? 2012. 90 f. Tese (Doutorado) - Economics, Wu Vienna University of Economics and Business, Viena, 2012. Disponível em: <<http://dev.economicsofbitcoin.com/mastersthesis/mastersthesis-surda-2012-11-19b.pdf>>. Acesso em: 06 nov. 2016.

THE ECONOMIST (from the print edition). **The trust Machine**, 31 out, 2015. Disponível em: <<http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>>. Acesso em: 08 mai. 2016.

ULRICH, F. **Bitcoin**: A moeda na era digital. São Paulo: Instituto Mises Brasil. 100p., 2014. Disponível em:
http://www.mises.org.br/files/literature/MisesBrasil_BITCOIN_BROCHURA.pdf. Acesso em: 08 mai. 2016.

VAN DER LAAN, C. **É crível uma economia monetária baseada em Bitcoins?** Limites à disseminação de moedas virtuais privadas (2014). Disponível em:
<http://www12.senado.gov.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td163>. Acesso em: 08 mai. 2016.